UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS
ESCOLA DE COMUNICAÇÃO

A ÉTICA HACKER NA ERA DO SIGILO DA INFORMAÇÃO

DIEGO GOMES DE SOUSA

RIO DE JANEIRO

2013

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

ESCOLA DE COMUNICAÇÃO

CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS

JORNALISMO

A ÉTICA HACKER NA ERA DO SIGILO DA INFORMAÇÃO

Diego Gomes de Sousa

Monografia de graduação apresentada à Escola de Comunicação da Universidade Federal do Rio de Janeiro, como requisito parcial para a obtenção do título de Bacharel em Comunicação Social, Habilitação em Jornalismo.

Orientadora: Profª Drª Cristina Rego-Monteiro da Luz

RIO DE JANEIRO

2013

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

ESCOLA DE COMUNICAÇÃO

TERMO DE APROVAÇÃO

A Comissão Examinadora, abaixo assinada, avalia a Monografia **A Ética Hacker na era do sigilo da informação**, elaborada por Diego Gomes de Sousa.

Monografia examinada:

Rio de Janeiro, no dia ...../...../.....

Comissão Examinadora:

_____

Orientadora: Prof.ª Drª Cristina Rego-Monteiro da Luz

_____

Prof.ª Drª Cristina Haguenauer

_____

Prof.ª Drª Marie Santini

RIO DE JANEIRO

2013

FICHA CATALOGRÁFICA

SOUSA, Diego Gomes de.

A Ética Hacker na era do sigilo da informação – Rio de Janeiro; UFRJ/ECO, 2013.

56 f

Monografia (Graduação em Comunicação Social/ Jornalismo) – Universidade Federal do Rio de Janeiro – UFRJ, Escola de Comunicação – ECO.

Orientação: Cristina Rego-Monteiro da Luz

1. Ética Hacker. 2. Internet. 3. Vigilância Cibernética. I. LUZ, Cristina Rego Monteiro da. II. ECO/UFRJ. III. Jornalismo. IV. A Ética Hacker na era do sigilo da informação.

SOUSA, Diego Gomes de. **A Ética *Hacker* na era do sigilo da informação**. Orientadora: Prof.ª Dr.ª Cristina Rego-Monteiro da Luz. Rio de Janeiro: UFRJ/ECO. Monografia em Jornalismo.

RESUMO

A sociedade humana vive hoje uma intensa acumulação de tecnologias, fazendo com que haja colossais diferenças de conhecimento e compreensão convivendo simultaneamente na contemporaneidade. Em um mesmo segmento onde parte da humanidade gira em torno da internet, há muitos equívocos e desconhecimento. Até hoje, parcelas significativas da mídia e de usuários da informática ainda veem pesquisadores do universo cibernético como criminosos. No entanto, eles são apenas curiosos que buscam melhores formas de fazer as coisas acontecerem. Este trabalho destina-se a entender e explicar as origens dos *hackers* e sua cultura, sua ética de trabalho, seu *modus operandi* e seus objetivos. Aborda-se a forma como essa ética se aplica ao contexto do pós 11 de setembro de 2001 e ao sigilo de informação, analisando os casos do WikiLeaks – *hackers* que trabalham para a ampla distribuição de conhecimento – e das denúncias de espionagem realizada pelo governo dos Estados Unidos, caso em que *hackers* trabalham para a distribuição de conhecimento para quem está no poder. Finalmente, procuramos identificar o papel da ética *hacker* nessas situações que fazem oposição uma a outra.

Palavras chave: Ética Hacker. Internet. Vigilância cibernética. WikiLeaks. NSA.

AGRADECIMENTOS

Agradeço aos meus pais, Maria das Graças e Alcides, pelo carinho e dedicação demonstrados ao longo desses 23 anos. Só eles sabem tudo que tiveram que enfrentar para que eu chegasse aonde eu cheguei. Agradeço ao meu irmão, Daniel, pela felicidade diária que proporciona desde o dia em que nasceu. Agradeço à Luana, a melhor namorada que existe e amor da minha vida. Agradeço aos meus amigos que estiveram ao meu lado nos momentos difíceis, como na produção desta monografia, e nos momentos de alegria. Não seria nada sem nenhum de vocês. Agradeço à Cristina Rego-Monteiro, minha orientadora e melhor professora da ECO. Agradeço também ao Clube de Regatas do Flamengo por ter conquistado a Copa do Brasil 2013 e me dado tranquilidade para concluir esta monografia.

SUMÁRIO

1. INTRODUÇÃO

No dia 05 de junho de 2013 uma notícia informou ao mundo que os Estados Unidos espionava seus próprios cidadãos sob a alegação de que estaria combatendo o terrorismo[1]. A informação revoltou a população e a imprensa norte-americana e de outros países. Nas semanas seguintes revelações vieram à tona: a Agência de Segurança Nacional norte-americana utilizava alta tecnologia para espionar cidadãos da China[2], Alemanha[3] e Brasil[4], além de seus governantes e empresas importantes. O responsável pelo vazamento de todas essas ações extremamente secretas foi um *hacker* chamado Edward Snowden[5]. O delator, que é um ex-analista de inteligência da NSA e tinha acesso irrestrito a diversos documentos da agência, tornou-se uma das grandes figuras do ano de 2013 e fez com que o governo de Barack Obama fosse extremamente criticado não só por manter um programa iniciado na gestão de George W. Bush em sua guerra ao terror pós-11 de setembro, mas também por ampliar os investimentos em tecnologia para espionagem e análise de dados. Snowden também suscitou um debate acerca da ética de seus atos. Ele é um traidor de sua própria nação ou um herói que revelou crimes que estavam sendo cometidos contra pessoas completamente insuspeitas? Ele é um *hacker*? Nesta condição é possível que ele pudesse agir eticamente? Os *hackers* são criminosos?

Este trabalho surgiu com a motivação de entender como os *hackers* atuam na sociedade em rede contemporânea, resgatando suas origens históricas no *Massachusetts Institute of Technology* (MIT), sua cultura disseminada antes mesmo do surgimento da internet, sua ética de trabalho, seu *modus operandi* e relevância no mundo movido pela ética capitalista – como conceituada pelo sociólogo Max Weber (2009) – e pela economia informacional, conceito criado pelo também sociólogo Manuel Castells (2000). Ele também é fruto de um desejo pessoal de estudar este mundo que sempre me pareceu ao mesmo tempo fascinante, misterioso e de certo modo inacessível. Além de Weber e Castells, foram utilizados textos de Steven Levy, Pekka Himanen, Pierre Lévy, Eric Raymond, Richard

[1] http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Acesso: 04 de dezembro de 2013.
[2] http://www.scmp.com/news/hong-kong/article/1259508/edward-snowden-us-government-has-been-hacking-hong-kong-and-china. Acesso: 04 de dezembro de 2013.
[3] http://www.spiegel.de/international/germany/nsa-spies-on-500-million-german-data-connections-a-908648.html. Acesso: 04 de dezembro de 2013.
[4] http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934. Acesso: 04 de dezembro de 2013.
[5] http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Acesso: 04 de dezembro de 2013.

Stallman e Chris Anderson. Notícias e artigos de jornais, revistas e portais que cobriram a repercussão dos vazamentos de documentos confidenciais pelo WikiLeaks e os casos de espionagem da NSA também foram utilizados na pesquisa. Os principais conceitos abordados na pesquisa são a ética *hacker*, a ética protestante e o espírito do capitalismo, a sociedade em rede, a cibercultura e o ativismo *hack*er.

No capítulo inicial é feito um resgate da história dos *hackers*, seu surgimento no Techmodel Railroad Club do MIT e posterior desenvolvimento no Laboratório de Inteligência Artificial do mesmo MIT. Através do *Arquivo de Jargões*, o dicionário definitivo da cultura *hacker*, procura-se explorar as origens da palavra *hacker* e o que ele é exatamente, além de entender qual foi o contexto histórico em que estes pesquisadores cibernéticos surgiram e como eles driblaram a escassa tecnologia disponível na época para divulgar sua cultura através de redes como a ARPANET, a precursora da internet como conhecemos hoje. Através das explicações de Richard Stallman, criador do sistema que originou o Linux, entendemos o que os *hackers* fazem e o que é um *hack*. A segunda geração de *hackers*, formada por nomes como Steve Jobs, Steve Wozniak e Bill Gates, responsáveis pelo surgimento dos computadores pessoais, também é estudada e tem sua história revisitada.

Ainda no primeiro capítulo é estabelecida a diferença entre *hackers* e *crackers*. Estes últimos sim, os criminosos virtuais que a mídia erroneamente rotula como *hackers*. A origem dos *crackers* também está no MIT. Quando os alunos do instituto precisaram burlar alguns sistemas de segurança para escrever suas linhas de código, eles estavam iniciando uma nova cultura baseada na invasão de sistemas. Alguns jovens, que não faziam parte do meio acadêmico e aprenderam a programar de forma autodidata, utilizaram seus conhecimentos para invadir sistemas por diversão e, em casos extremos, roubar de dados e dinheiro via computador. Um destes grupos, chamado *The 414s*, ganhou destaque no início dos anos 80 e a Cultura *Hacker* foi parar na mídia, ainda que retratada de forma equivocada. Insatisfeitos pelas comparações indevidas, os *hackers* que não estavam envolvidos em atividades ilícitas criaram o termo *cracker* para acabar com as associações feitas pela mídia e por leigos entre os dois grupos.

O capítulo termina tratando da Ética *Hacker*, tema principal deste estudo. A partir de Steven Levy (1984), que estabeleceu quais são as atitudes e princípios que permeiam os *hackers* éticos: basicamente a liberdade de informação e expressão, não-preconceito e o entendimento de que computadores podem mudar vidas. A partir da obra de Pekka Himanen é analisado como a ética *hacker* entra no contexto da Era da Informação e qual é a relação dos

hackers com o trabalho e com as variáveis importantes decorrentes dele, como tempo e dinheiro. Procura-se entender quais são as motivações de um *hacker*, porque ele é o que é e o que o mobiliza.

No segundo capítulo é dado um passo atrás para que possamos entender, através de uma linha do tempo, por que a Era da Informação tornou-se a Era do sigilo da informação. Boa parte das novas invenções na área da tecnologia da informação foram criadas para serem utilizadas no combate ao terrorismo ou na guerra. Através de notícias da época e artigos de publicações especializadas, veremos como a tecnologia se desenvolveu e vem trazendo para o campo virtual o que antes acontecia nos campos de batalha. Decretos como o *Patriot Act*, que permitem o acesso a comunicações eletrônicas de suspeitos sem emissão de uma ordem judicial, e o incentivo ao ensino de linguagens de programação, mostram como o governo dos EUA pretende criar uma nova geração de *hackers* comprometida com o combate ao terrorismo.

Neste capítulo abordaremos um primeiro estranhamento entre *hackers* e o governo, e o *Big Data*, ferramenta para analisar grandes volumes de dados, que mostra como é simples monitorar os passos de qualquer pessoa atualmente, deixando de lado o pensamento científico e humanístico, uma das bases da atuação *hacker*.

O terceiro capítulo fala sobre o WikiLeaks, um dos estudos de caso desse trabalho. A atuação do WikiLeaks foi fundamental para a denúncia de diversos crimes cometidos nas guerras do Iraque e Afeganistão e para tornar públicos diversos telegramas diplomáticos dos Estados Unidos, assim como outros documentos de governos e corporações de alto interesse público. Expor documentos e informações confidenciais passa, segundo a ética *hacker*, pela questão da liberdade de informação. Veremos também que a atitude *hacker* pode estar presente em outras áreas de atuação que não sejam a informática. Neste caso, no jornalismo.

Os *hackers* do jornalismo, como proposto por Mancini (2011), são profissionais que pensam novas maneiras para revolucionar as redações e fazer com que o jornalismo volte a se destacar como o importante ator social que é.

Por fim, o último capítulo tem como foco a relação vigente entre um *hacker* como Snowden e seu governo e as recentes acusações de espionagem dirigidas ao governo dos Estados Unidos, segundo as quais a NSA, Agência Nacional de Segurança, estaria espionando cidadãos, empresas e governos. São examinadas hipóteses para identificar os motivos pelos quais os Estados Unidos procuraram *hackers* para compor suas agências federais de inteligência, quais foram as estratégias para isso e o que os *hackers* pensam sobre trabalhar

para quem está no poder, levando-se em consideração quais são as implicações dessa situação sobre os valores identificados como seu pensamento ético.

Em seguida a história da NSA é contada, desde seu surgimento até as denúncias que culminaram na impopularidade vivida pela agência atualmente e como a vigilância era feita. Através das notícias e artigos sobre os casos de espionagem procuramos entender quais foram os impactos na comunidade *hacker* e como eles estão vendo as agências federais de inteligências no momento.

Ainda no quarto capítulo, mostramos quem é Edward Snowden e o que ele pretendia quando viajou para Hong Kong e delatou a NSA para os jornalistas Glenn Greenwald e Laura Poitras.

Para finalizar o trabalho, veremos que a atuação da NSA não é individual, que ela conta com agências de outros países e que seu trabalho se deu até no Brasil. Aqui, Dilma Rousseff e a Petrobras foram identificadas como vítimas da espionagem digital norte-americana.

Nas considerações finais são apresentadas algumas ideias que pudemos depreender da ética *hacker* na contemporaneidade. Também são apontados, brevemente, possíveis caminhos para a continuidade das investigações sobre o tema, visto que é um assunto extremamente atual e relevante para pesquisa.

2. *HACKERS*

O termo *hacker* vem do verbo "*to hack*", que significa literalmente "cortar". Um *hacker* pode ser alguém que corta ou a pessoa que faz ferramentas. Os *hackers* de computador foram equivocadamente vistos por muitos anos como piratas e/ou criminosos virtuais, pessoas sem rosto que agem secretamente se escondendo atrás de cabos, fios, redes e protocolos. O medo da tecnologia, o surgimento da internet e da web no início dos anos 90 causaram uma aversão aos *hackers*, mas, quando estudantes do *Tech Model Railroad Club* e do Laboratório de Inteligência Artificial do *Massachussets Institute of Technology* (MIT) passaram a usar o termo nos anos 60, eles só queriam dar vida a uma cultura que estava nascendo entre programadores e entusiastas da informática no meio acadêmico.

2.1. A cultura *Hacker*

O *Tech Model Railroad Club* é uma organização de estudantes do MIT e um dos clubes de ferromodelismo mais importantes do mundo. Apesar de não estar ligado diretamente à informática, foram integrantes do clube que criaram o termo *hack* ainda nos anos 50. Segundo o TMRC, o *hack* é uma solução simples e inteligente, que não altera o sistema onde ele é inserido[6] - no contexto do ferromodelismo, onde se trabalha com um sistema de controle dos trens, o *hack* é muito utilizado para criar soluções alternativas a problemas que não são resolvidos das formas tradicionais. Um exemplo dado por Steven Levy é roubo de diodos e outros componentes eletrônicos que os integrantes do TMRC praticavam sempre que precisavam trocar componentes danificados. Para eles, este roubo não é errado, já que para solicitar esses diodos demandaria uma burocracia que eles preferiam contornar. A melhor forma de acelerar o processo era esperar anoitecer e pegar as peças nos armários onde ficavam guardadas. Assim surgiu o Comitê de Requisições da Madrugada (LEVY, 1984). Orgulhosos do termo que ajudaram a espalhar pelo mundo e da cultura que nasceu em seu berço, o TMRC não aceita o uso da palavra *hacker* para os criminosos que invadem redes e computadores para roubar dados. Para eles estas pessoas são ladrões ou *crackers*[7], termo que será explicado adiante. A realidade da programação chegou ao TMRC em 1961, quando o

6 http://tmrc.mit.edu/hackers-ref.html. Acesso: 20 de setembro de 2013.
7 Ibidem.

MIT adquiriu o computador PDP-1[8]. Logo, os integrantes do clube começaram a criar ferramentas de programação e gírias que culminaram no surgimento da Cultura *Hacker*[9]. Após o entusiasmo inicial com o PDP-1 no TMRC, os programadores do Laboratório de Inteligência Artificial do MIT passaram a se dedicar mais aos *hacks*, criando novas linguagens e aprimorando as que já existiam. A criação do TX-0[10], o sucessor do PDP-1, foi fundamental para o desenvolvimento da cultura *hacker*. Este computador, também conhecido como *tixo*, permitia que os programadores vissem as linhas de código sendo executadas no momento em que eram escritas. Ele foi responsável pela criação de programas depuradores e editores de texto.

O passo seguinte para a disseminação da cultura *hacker* foi o surgimento da ARPANet[11], a primeira rede transcontinental de alta velocidade que foi o protótipo do que viria a ser a internet como conhecemos hoje. Ela foi criada pelo Departamento de Defesa dos Estados Unidos para interligar e facilitar as comunicações entre bases militares e departamentos de pesquisa norte-americanos durante a Guerra Fria. Muitos destes departamentos de pesquisa ficavam em universidades e os *hackers*, que até então faziam parte exclusivamente do meio acadêmico, começaram a trocar informações entre si. A ferramenta colaborou para intensificar a troca de informações e conhecimento entre as universidades e a difundir a cultura ciber e os termos dessa cultura. As primeiras discussões sobre a ideologia *hacker* foram feitas através da ARPANet. Entre 1973 e 1975, gírias, termos e jargões *hackers* foram criados e compartilhados através da rede. Mais tarde, eles foram compilados no "Arquivo de Jargões"[12], glossário *hacker* que segue atual até os dias de hoje e foi consultado diversas vezes para este trabalho.

O "Arquivo de Jargões" define o *hacker* como alguém que programa entusiástica e obsessivamente ou apenas alguém que prefere criar projetos práticos em vez de teorizar sobre

---

8 Programmed Data Processor-1. Computador criado Digital Equipmente Corporation em 1959, com uma memória de pouco mais de 9 mil bytes e 200 kilohertz de frequência, levando 10 microsegundos para realizar um cálculo aritmético.

9 http://www.catb.org/esr/writings/homesteading/*hacker*-history/ar01s02.html. Acesso: 21 de setembro de 2013.

10 Transistorized Experimental computer zero. Foi o primeiro computador construído com transistores e tinha uma memória de 64 mil bytes, número incrível à época.

11 http://www.catb.org/esr/writings/homesteading/*hacker*-history/ar01s02.html. Acesso: 21 de setembro de 2013.

12 "*The Jargon File*" é um glossário organizado pelo *hacker* e escritor Eric Raymond e ficava hospedado no endereço www.tuxedo.org/~esr/jargon. No entanto, a URL direciona para a página inicial do portal, onde se encontra uma homenagem a Aaron Swartz, famoso por ser co-autor da especificação RSS e do site Reddit. Aaron foi encontrado morto em seu apartamento no dia 11 de janeiro de 2013 após ter sido condenado pela justiça americana pelos crimes de invasão de computadores e por compartilhar arquivos acadêmicos em domínio público. O Jargon File está disponível atualmente em www.catb.org/~esr/jargon/ e também foi lançado em livro com o nome *The Hacker's Dictionary.*

o assunto[13]. Já uma definição mais moderna do termo, foge do entendimento universal de que para ser um *hacker* é obrigatório ser da área de informática ou, ao menos, da tecnologia. Um *hacker*, nesse contexto, é um entusiasmado e criativo pesquisador de campo.

> Faz algo para melhorar ou alterar o funcionamento de um sistema com uma solução criativa ou não convencional. *Hackers* são pessoas que buscam excelência em sua profissão através de métodos pouco ortodoxos, inexplorados ou inovadores (MANCINI, 2011, p. 15).

Burrell Smith, criador do *Macintosh*, falou na primeira Conferência *Hacker* em 1984 que "você pode ser um carpinteiro *hacker*. Não é necessariamente alta tecnologia. Tem a ver com sua habilidade e sua preocupação de se importar com o que faz" (LEVY, 1984, p. 484, tradução nossa). Já Eric Raymond diz que "existem pessoas que colocam a atitude *hacker* em outras coisas [que não sejam *software*], como eletrônica e música – na verdade, você pode encontrar a atitude *hacker* nos melhores tipos de ciências e artes" (RAYMOND, 1999, p. 32, tradução nossa).

Richard Stallman, *hacker* e programador famoso pela criação do sistema operacional GNU[14] e da Fundação para o *Software* Livre[15], conta que durante um encontro de entusiastas do GNU na Coreia do Sul, em junho de 2000, ele utilizou seis *hashis*, três em casa mão, para fazer sua refeição. Apesar de ser muito mais difícil comer com seis *hashis* em vez de dois, ele diz que justamente pelo nível de dificuldade e por ninguém nunca ter pensado nisso antes, sua manobra tem "*hack value*"[16]. O "*hack value*" é a motivação para investir tempo e esforço em um trabalho que parece não ter utilidade explícita, mas o *hacker* o faz apenas por saber que está empreendendo seus conhecimentos em um hack[17]. Stallman utiliza esta história para ilustrar sua visão do que é um *hacker*. Para ele, fazer uma coisa difícil de forma divertida, independente de ser algo útil ou não, é hackear.

> É difícil escrever uma definição simples de algo tão variado como o ato de hackear, mas eu acho que estas atividades têm em comum o lúdico, a

13 "*The Jargon File*", em *hacker*.
14 Sistema operacional criado por Richard Stallman e que ainda não tem nenhuma versão estável. Começou a ser idealizado em 1984 e em 1991 estava quase pronto, mas não tinha um núcleo. Linus Torvalds criou um núcleo e utilizou toda a estrutura do GNU para dar vida ao Linux.
15 Organização sem fins lucrativos criada por Richard Stallman em 1985 para se dedicar ao fim do controle sobre cópias e redistribuição de *software*. A fundação se dedica a estudar e modificar programas de computador para que qualquer pessoa possa ter acesso gratuito a todo tipo de *software*. A FSF patrocina o projeto GNU.
16 http://stallman.org/articles/on-hacking.html. Acesso: 21 de setembro de 2013.
17 http://stallman.org/articles/on-hacking.html. Acesso: 21 de setembro de 2013.

> sagacidade e a exploração. Portanto, hackear significa explorar os limites daquilo que é possível, com um espírito de sagacidade lúdica. Atividades que mostram essa sagacidade lúdica têm "valor *hacker*".[18]

Há uma segunda geração de *hackers* que ganhou força com a invenção dos computadores pessoais. Quando o Altair 8800[19] foi criado, em 1975, Gordon French[20] e Fred Moore[21] criaram o *Homebrew Computer Club*, um clube de entusiastas da informática que se reuniram de março de 1975 a dezembro de 1986. A proposta era manter um fórum para interessados em tornar os computadores mais acessíveis para as pessoas. Dos encontros do *Homebrew Computer Club*, surgiram grandes *hackers* e nomes importantes da Tecnologia da Informação, como Steve Wozniak, Steve Jobs e Bill Gates. O computador *Apple-1* foi criado por Wozniak como um dos projetos do grupo em 1976 e a ideia de vendê-lo partiu de Steve Jobs. O *Homebrew Computer Club* também foi essencial para o surgimento da cultura do Vale do Silício, região dos Estados Unidos com as maiores empresas de tecnologia do mundo, como a própria *Apple*, *Google*, *Facebook*, *Intel* e outras. A *Microsoft* nasceu no Vale do Silício, mas hoje fica em Redmond, Seattle.

2.2. *Hackers* x *Crackers*

Uma atitude que está no cerne de toda ação *hacker* é não acatar as regras e padrões estabelecidos, por isso eles buscam caminhos e soluções alternativas para trazer ao mundo real suas ideias ou apenas para quebrar os paradigmas que se impõem sobre seu trabalho. Os *hackers* não são uma confraria, ou seja, não necessariamente trabalham sempre em conjunto – apesar de terem nascido em grupos acadêmicos como TMRC e o Laboratório de Inteligência Artificial do MIT e, posterioramente, terem surgido grupos como o *Homebrew Computer Club*. Existem *hackers* que não são ligados à organizações e fazem todo seu trabalho de forma solitária, em seus computadores pessoais em suas residências. Esta "anarquia" do mundo *hacker*, que é heterogêneo, sem liderança e descentralizado, é o que permite seu

18 Ibidem. Tradução nossa do original: "*It is hard to write a simple definition of something as varied as hacking, but I think what these activities have in common is playfulness, cleverness, and exploration. Thus, hacking means exploring the limits of what is possible, in a spirit of playful cleverness. Activities that display playful cleverness have 'hack value'*".

19 Computador criado em 1975 e vendido pela revista Popular Electronics. Fez muito mais sucesso que o esperado e hoje é considerado como a maior motivação para a criação do computador pessoal.

20 Programador e Engenheiro da Computação.

21 Ativista político. (1941-1997)

desenvolvimento contínuo e a constante quebra de paradigmas na busca por alternativas e no desafio àqueles que tentam impor métodos ou retêm informação para si.

Os *hackers* especialistas em quebra de segurança também surgiram no MIT. Quando os computadores do instituto começaram a apresentar algumas restrições de acesso aos usuários, os *hackers* criaram maneiras de burlar o sistema para utilizar os equipamentos sem preocupações de restrição e também apenas pelo *hack value* de invadir um sistema e modificar suas configurações de segurança. O desejo do Laboratório de Inteligência Artificial do MIT não era se preocupar em "quebrar" a segurança de computadores e sim que não houvesse segurança alguma. O mais importante era o uso da plataforma ser livre para qualquer usuário.

Pensando nisso, os integrantes do laboratório criaram o sistema operacional Incompatible Timesharing System[22], feito para funcionar nos computadores PDP-6s e PDP-10s. Eric Raymond diz que os ITS foram criados porque os alunos do MIT queriam um sistema que funcionasse do jeito que eles quisessem e, para sorte de todos, "o MIT tinha inteligência suficiente para suprir sua arrogância"[23].

Até hoje o ITS é venerado por alguns *hackers*. Apesar de ter sido um sistema operacional idiossincrático e programado em Assemble, linguagem que não permitia muitos avanços tecnológicos, ele foi responsável por quebrar as correntes que o sistema anterior impunha através das suas configurações de segurança. O ITS foi responsável por inovações como compartilhamento de arquivos realizado de maneira transparente e terminais independentes de entrada e saída. Após a desativação do último computador com ITS do MIT, em maio de 1990, vários *hackers* passaram a admirar o Incompatible Timesharing System. Há os que consideram o sistema o melhor de todos os que foram criados. Estas pessoas são chamadas de trogloditas[24] no meio *hacker*.

No início dos anos 80, a cultura *hacker* do MIT já estava estabelecida nos meios acadêmico e militar e boa parte de seus jargões já haviam sido cunhados. Apesar dos *hackers* existirem a duas décadas, somente em 1983 eles ganharam os holofotes da mídia, e isso aconteceu através de um grupo especialista em quebra de segurança chamado *The 414s*. O grupo era formado por jovens *hackers* de Milwaukee, Winscosin – o nome *The 414s* vem do código telefônico da região – que ficaram famosos após invasões a sistemas de organizações

22 O nome do sistema é uma brincadeira com seu antecessor, o Compatible Time-Sharing System, que tinha diversas configurações de segurança.
23 http://www.catb.org/esr/writings/homesteading/*hacker*-history/ar01s02.html. Acesso: 25 de setembro de 2013.
24 http://www.catb.org/~esr/jargon/html/T/troglodyte.html. Acesso: 25 de setembro de 2013.

norte americanas importantes, como o Laboratório Nacional de Los Alamos, o Memorial do Câncer Sloan-Kettering e o banco Security Pacific[25].

O grupo *The 414s* foi matéria em veículos do porte do New York Times, Newsweek e a revista Time devido aos seus feitos e também foi alvo de investigações do FBI. Foi provado que as ações dos jovens *hackers* causaram alguns prejuízos ao Memorial Sloan-Kettering. A mídia passou a tratar todo invasor de sistemas como *hacker* e os programadores do MIT não gostaram de serem comparados a pessoas mal intencionadas e/ou jovens inexperientes que utilizavam seus conhecimentos de informática para invadir sistemas, aproveitando falhas de segurança e não fazendo uso de suas capacidades cognitivas de codificar e decodificar diversas linhas de linguagem de programação.

Dessa insatisfação os próprios *hackers* cunharam o termo *cracker* em 1985[26] para se referir exclusivamente aos invasores de sistema. Atualmente, *cracker* é o termo utilizado comumente para designar criminosos virtuais que invadem sistemas e computadores pessoais para roubar dados e senhas. As invasões realizadas para mostrar como um sistema é desprotegido ou enviar mensagens – normalmente de cunho político – não são mais associadas a *crackers*. O grupo anarquista e ciberativista Anonymous faz uso dessa estratégia para tirar do ar *sites* de instituições contrárias ao seu pensamento libertário ou para enviar mensagens sobre seus atos.

Segundo o Arquivo de Jargões, em 1981 os *hackers* tentaram chamar os invasores de sistema de "*worms*"[27], mas o termo não se popularizou[28]. O jargão *cracker* começou a ser utilizado porque o neologismo representava não só a atitude de quem invadia um sistema (*safe-cracker*), mas também a repulsa que os *hackers* sentiam. Explico: no inglês antigo, *cracker* é o termo utilizado para se referir a uma pessoa desagradável – a palavra aparece até mesmo no drama de Shakeaspeare Vida e Morte do Rei João[29] – e no inglês coloquial dos Estados Unidos é um sinônimo para a ofensa "*white trash*"[30].

O Arquivo de Jargões também deixa claro que todo *hacker* possui conhecimentos suficientes para invadir um sistema seguro, mas que ele só faz isso em seu "estágio de larva"[31] - este é o período pelo qual todo *hacker* passa quando está começando a hackear e/ou

25 http://www.computerworld.com/s/article/9130828/Hackers_steal_legislators_attention. Acesso: 01 de dezembro de 2013.
26 http://www.catb.org/~esr/jargon/html/C/cracker.html. Acesso: 25 de setembro de 2013.
27 Vermes.
28 http://www.catb.org/~esr/jargon/html/C/cracker.html. Acesso: 25 de setembro de 2013.
29 http://www.catb.org/~esr/jargon/html/C/cracker.html. Acesso: 25 de setembro de 2013.
30 Tradução: lixo branco. É um termo depreciativo utilizado para se referir a pessoas brancas de classes sociais baixas. Chamar uma pessoa de *white trash* é dizer que ela não tem conhecimentos culturais e econômicos.
31 http://www.catb.org/~esr/jargon/html/L/larval-stage.html. Acesso: 25 de setembro de 2013.

estudando novas linguagens de programação ou sistemas operacionais. Nesse estágio, o *hacker* passa dias inteiros programando de forma ininterrupta, sem dormir, comer e até mesmo sem fazer a própria higiene pessoal. O estágio de larva pode durar de seis meses a dois anos - ou quando for realmente necessário para a realização de um trabalho. Um *hacker* deve ter conhecimentos que vão além de saber explorar falhas de segurança e de testar padrões de senhas. Ele deve direcionar sua inteligência em decodificar linguagens complexas de programação e dedicar tempo para criar novas linguagens. Acima de tudo, um *hacker* deve compartilhar seu conhecimento com outros.

2.3. A Ética *Hacker*

A primeira vez que o termo "Ética *Hacker*" foi utilizado, foi em 1984, no livro "*Hackers: Heroes of the Computer Revolution*", do jornalista e Steven Levy. O autor destrincha seis princípios que movem a cultura *hacker* desde a época do TMRC. Mesmo nos anos 60 quando o TX-0 ainda era uma novidade para o MIT, as plataformas da Ética *Hacker* já estavam montadas (LEVY, 1984). Os princípios da Ética *Hacker* são: acesso aos computadores – e qualquer coisa que possa ensinar algo sobre como o mundo funciona – deve ser ilimitado, toda informação deve ser livre, desconfiar das autoridades e promover sua descentralização, julgar os *hackers* somente por suas habilidades de programação – não por critérios como formação, idade, raça ou classe social –, computadores podem criar arte, computadores podem mudar vidas para a melhor.

Levy (Ibidem) entende que o mundo seria muito melhor se todas as pessoas pudessem e soubessem usar computadores a seu favor como os *hackers* fazem, ou seja, sendo curiosas, céticas, questionando poderes estabelecidos e sua burocracia, interagindo com máquinas de forma produtiva, criativa e sem julgamentos.

Os *hackers* são pessoas que programam de forma obsessiva. Deixam de fazer qualquer outra coisa por dias, apenas para programar em uma nova linguagem ou sistema operacional. Hackear é procurar a melhor forma de fazer seu trabalho, utilizando a inovação e métodos não convencionais. Mas por que eles fazem isso? Qual é a motivação por trás de milhares de linhas de código escritas compulsivamente? Segundo Linus Torvalds (2001), criador do sistema operacional Linux, a motivação *hacker* é, basicamente, diversão.

Torvalds criou a *Linus's Law* quando deu uma palestra na Universidade da Califórnia, sobre os desafios da sociedade conectada em rede. Basicamente, a Lei de Linus diz que tudo

que o ser humano faz é motivado por três fatores: sobrevivência, vida social e entretenimento. Conforme a sociedade evolui, as coisas também podem mudar de um fator para outro. O sexo, que, em teoria, serve apenas para reprodução – logo, sobrevivência –, também é um importante meio de criar vínculos e manter a sociabilidade, além de ser uma forma de entretenimento em diversas culturas. De acordo com Torvalds, a motivação do *hacker* já passou pelos dois primeiros estágios e está na fase do entretenimento. Passar dias programando não é um motivo de sobrevivência, não é dali que um *hacker* tira seu sustento e tal atividade também diminui sua vida social, já que ele faz tudo sozinho. É o sentimento de estar criando algo novo que faz os *hackers* "se coçarem".

Para Pekka Himanen, paixão é a palavra mais adequada para descrever a motivação *hacker*, porque "a paixão transmite mais intuitivamente os três níveis da filosofia Unix[32] – a dedicação a uma atividade que é intrinsicamente interessante, inspiradora e alegre" (HIMANEN, 2001, p. 6, tradução nossa). A paixão que move os *hackers* é a mesma que movia os filósofos pós-socráticos do período clássico da Grécia Antiga. E é a paixão que dá o tom da ética do trabalho *hacker*. Himanen estabelece um interessante contraponto da ética do trabalho *hacker* com o livro A Ética Protestante e o Espírito do Capitalismo, do sociólogo alemão Max Weber.

Vale pontuar que a motivação primária dos *hackers* é a que menos garante a sua sobrevivência. No entanto, podemos notar que a lógica da motivação *hacker* segue o caminho contrário da Linus's Law. A própria criação de Linus Torvalds, o Linux, comprova isso. O principal motivo do sistema operacional fazer tanto sucesso – e hoje ser uma importante figura de mercado ao lado do Windows e do MacOS –, é o fato de ser customizável e também poder ter constantes atualizações feitas por qualquer pessoa. Quando alguma modificação é feita no Linux, logo ela é compartilhada na rede para que outros *hackers* possam testá-la, criticá-la e aprimorá-la. A evolução do Linux passa pelo conceito de *inteligência coletiva* do filósofo francês Pierre Lévy. A inteligência coletiva é "uma inteligência distribuída por toda parte, incessantemente valorizada, coordenada em tempo real, que resulta em uma mobilização efetiva das competências" (LÉVY, 1998. p. 17, tradução nossa). Assim, o que começa como entretenimento (ou paixão) passa para o nível da sociabilidade. Segundo Eric Raymond (1998), para um *hacker*, obter reconhecimento de uma comunidade que compartilha da mesma paixão que ele é muito mais importante do que ganhar dinheiro com seu trabalho. Para os *hackers*, a *sociabilidade* chega naturalmente quando o produto que é fruto da sua

32 Em The Art of Unix Programming (2003), Eric Raymond diz que para estar de acordo com a filosofia do sistema operacional você precisa se importar, precisa brincar com ele e precisa querer explorá-lo.

diversão ganha vida. São etapas de um fluxograma inverso do que é esperado e que termina na *sobrevivência*. Na realidade "mundana"[33], ou seja, daqueles que não fazem parte da indústria da computação, a vida social surge como consequência da sobrevivência – o trabalho – e expõe a falta de entretenimento e de diversão fora dos seus círculos de colegas de trabalho. O modelo de vida social dos *hackers* é muito poderoso e coeso, derrubando a máxima de que *hackers* são pessoas solitárias. Marvin Minsky, membro do laboratório de Inteligência Artificial do MIT, diz que "ao contrário do senso comum, *hackers* são muito mais sociáveis que outras pessoas" (BRAND, *apud* HIMANEN, p.52).

Finalmente chegamos à fase da sobrevivência. Considerando que dinheiro pode comprar sobrevivência, podemos afirmar que este é o último estágio de motivação *hacker* já que seu "produto", após ser criado por diversão e testado por outros *hackers* de seu meio social, pode ser comercializado para garantir sua subsistência.

A relação dos *hackers* com dinheiro é semelhante à de qualquer outra pessoa. Apesar de serem libertários, os *hackers* sabem que precisam de dinheiro para sobreviver e utilizam sua paixão para isso. Fazendo um trabalho que é genuinamente apaixonado e que permite que a autogestão do tempo, é perfeitamente possível e aceitável tornar-se um "*hacker* capitalista". É o caso de Bill Joy e Andreas "Andy" Bechtolsheim, fundadores da Sun Microsystems. Fundada em 1982 para produzir estações de trabalho ligadas em rede, a empresa cresceu e se tornou uma gigante da informática mundial. Posteriormente, Bechtolsheim deixou a Sun para criar a Cisco Systems, fabricante de roteadores.

Steve Wozniak, co-fundador da Apple, foi um que também experimentou o gosto do capitalismo, mas por poucos anos. Wozniack se aposentou após seis anos da fundação da "Grande Maçã" da informática, com uma fortuna avaliada em cem milhões de dólares. Ele se tornou uma espécie de mentor de novos *hackers*, ensinando crianças em idade escolar a usar computadores. "Eu tenho contadores e secretários que cuidam dos meus negócios, para que eu possa passar quanto tempo quiser fazendo o que eu gosto, que é trabalhar com computadores, escolas e crianças" (WOLFSON; LEYBA, *apud* HIMANEN, 2001, p. 55, tradução nossa).

Um caso que destoa dos apresentados acima é o de Bill Gates, fundador da Microsoft. Ex-membro do *Homebrew Computer Club*, Gates fundou uma das grandes empresas de informática do mundo e se tornou o oposto de tudo que um *hacker* pode ser. A busca por lucro e o combate extremo à pirataria mostraram que Bill Gates tinha um espírito muito mais protestante do que *hacker*.

33 http://www.catb.org/~esr/jargon/html/M/mundane.html. Acesso: 03 de outubro de 2013.

As raízes da ética do trabalho *hacker* são acadêmicas, fazem parte do compartilhamento do conhecimento e do aprimoramento das técnicas, afim de que todos possam utilizá-las. Já a ética protestante tem raízes nos mosteiros, onde os monges não questionavam todo tipo de trabalho sem questionar os motivos de fazê-los (HIMANEN, 2001).

A ética católica pré-reforma pregava que o paraíso seria o local de descanso e regozijo eterno e o inferno o local onde os pecadores passariam a eternidade fazendo trabalhos forçados, que não resultariam em nada. A ética protestante, que teve os mosteiros como berço, subverteu esse pensamento e os cristãos pós-reforma só garantiriam um lugar no céu caso fizessem do trabalho a motivação de sua existência. Mesmo no céu eles teriam que trabalhar, para que a benção fosse completa[34]. Vale ressaltar que a ética protestante permeia a sociedade até hoje, mesmo entre as pessoas de outras religiões ou ateus.

Caso os *hackers* tivessem que escolher entre as duas éticas apresentadas acima, provavelmente eles ficariam ao lado da ética pré-protestante. No entanto, a ética do trabalho *hacker* não almeja que no fim da vida vamos passar a eternidade fazendo nada. A meta *hacker* não é ir para o Paraíso e sim colocar suas paixões no mundo, assim como suas linhas de código, seus softwares e seus sistemas operacionais. Para Manuel Castells (2000) o trabalho continuará sendo o núcleo da vida das pessoas no futuro próximo. A ética *hacker* está caminhando para romper com essa visão de que o trabalho pelo trabalho é o que mais importa. Himanen diz que, nesse contexto, "todos os *hackers* são *crack*ers, porque eles querem quebrar (*crack*) o cadeado da jaula de ferro[35]" (HIMANEN, 2001, p. 13, tradução nossa). A jaula de ferro do capitalismo faz com que o trabalho seja o centro da vida dos indivíduos ao mesmo tempo em que o isola de tudo mais que é importante. Nela, faltar a um dia de trabalho por estar doente pode ser um grande problema e a meta de vida que se tem é fazer o melhor serviço possível, deixando de lado compromissos pessoais, o lazer, família e amigos em segundo plano. Dentro dessa jaula, os patrões não precisam comandar de perto, já que tudo flui naturalmente pela própria vontade dos empregados, e sindicatos têm bem menos força do que em locais em que há abusos flagrantes de poder e desrespeito às leis de trabalho.

Talvez a melhor ferramenta que os *hackers* possuem para se afastar dessa visão de mundo é o tempo. Mais precisamente, como eles utilizam o tempo. Os *hackers* não costumam

34 O teólogo Johann Kasper Lavater diz que temos que trabalhar no Paraíso: "We cannot be blessed without having occupations. To have an occupation means to have a calling, an office, a special, particular task to do". *Aussichten in die Ewigketi* (1773), 3:93.

35 Metáfora de Weber em A Ética Protestante (pp. 181-183) que diz que o espírito do capitalismo se separou da ética Protestante e passou a funcionar sob suas próprias leis, tornando-se uma jaula de ferro neutra a religião.

programar em horário comercial, eles fazem isso em seu tempo livre ou quando bem entendem, porque a base de tudo é o entretenimento. Hackear não é visto primeiramente como trabalho e sim como hobby, para ser feito durante o tempo livre. Pekka Himanen (2001) diz que Linus Torvalds programou a primeira versão do Linux durante a madrugada e, algumas vezes, deixava o sistema operacional de lado para criar coisas diferentes no computador.

Como a ética protestante é totalmente voltada ao trabalho, sua relação com o tempo é a máxima estabelecida por Benjamin Franklin: tempo é dinheiro. Unidades de tempo cada vez menores são transformadas em dinheiro. É a otimização do tempo (HIMANEN, 2001, p. 21). De acordo com Castells (2000), estamos vivendo na era da "Economia informacional". Nela, os produtos que consumimos são informação ou a própria tecnologia da informação. A Economia Informacional é o que permite que vejamos o consumo como uma experiência e nos engajemos com corporações. O engajamento com as marcas e o consumo como uma experiência transcendental são estratégias realizadas por diversas empresas e que ficaram muito mais fáceis de serem disseminadas com as redes sociais. Estas estratégias são uma forma de conquistar os consumidores sem, necessariamente, oferecer um novo produto. Pekka Himanen diz que "as velozes mudanças tecnológicas tornam imperativa a oferta de novas tecnologias aos consumidores, antes que o concorrente o faça" (HIMANEN, 2001, p. 22, tradução nossa). No entanto, é possível compreender que é muito mais fácil vender seu produto como algo transcendental para que não seja necessário estar pesquisando e criando novas tecnologias a esmo.

Mancini (2011) diz que os meios de comunicação estão mudando a forma como oferecem seus produtos. Antes, se os jornais eram lidos pela manhã e a televisão era assistida à noite, hoje não há mais essa delimitação de tempo. É a passagem do *"prime time*" para o *"in between time"* do consumo de informação. Para que possamos consumir informação em nosso *in between time*, precisamos de tecnologias como *smartphones*, *tablets* e computadores com internet disponíveis 24 horas por dia - e não somente no horário de trabalho. Dessa forma, utilizamos essas tecnologias acreditando estar vivendo uma experiência única de ter acesso a entretenimento e informação a qualquer hora do dia, mas acabamos ficando mais presos ao trabalho. A facilidade de ter um smartphone nos faz tomar atitudes como responder e-mails aos fins de semana como se fosse algo natural. A partir disso, muitos empregadores passam a exigir de seus funcionários que façam atividades relacionadas a trabalho fora de seu expediente, muitas vezes oferecendo as ferramentas necessárias para isso.

A ética Protestante prega que não deve haver diversão no horário de trabalho e, cada vez mais, coloca trabalho no tempo livre dos indivíduos para que haja a sensação de pertencimento a uma suposta elite (HIMANEN, 2001). Os *hackers* não seguem essas regras. Como exemplificado anteriormente com Torvalds e a criação do Linux, eles têm uma relação completamente diferente com o tempo. Como a motivação inicial de todo *hacker* é o entretenimento, é certo dizer que praticamente todos os seus projetos começam a ser realizados no tempo livre, ou seja, nos fins de semana e/ou à noite. Os *hackers* deixam seus projetos de lado para se divertirem no computador ou passar um dia inteiro longe dele. "A visão *hacker* é que o uso de máquinas para otimização e flexibilizaçao do tempo deve levar os seres humanos a uma vida menos 'maquinocêntrica'" (Ibidem, p. 33, tradução nossa).

Mais uma vez, podemos estabelecer uma relação entre os *hackers* e a Academia e traçar um paralelo da relação entre a ética Protestante e os mosteiros. A auto-organização do tempo remete a Platão, que cunhou o termo *skhole*[36] para se referir às pessoas livres que poderiam utilizar seu tempo para trabalhar ou para ter tempo livre e relaxar. Já São Bento propõe um padrão para a vida nos mosteiros, ele diz que os salmos devem ser lidos repetidamente "pelas mesmas horas até o domingo, conservando-se de maneira uniforme e todos os dias a disposição dos hinos" [37].

A ética *hacker* questiona os horários fixos de trabalho porque eles impedem a criatividade do indivíduo, determinando que ele deve criar somente em horário comercial – ou fora do horário de trabalho, sem que seja devidamente remunerado por isso. O horário de trabalho também coloca pessoas adultas como crianças que precisam ser vigiadas ao longo de oito horas durante todos os dias para que não façam nada diferente do que está previsto no roteiro laboral. "*Hackers* não concordam com o ditado 'tempo é dinheiro', mas sim com o ditado 'essa é minha vida'. E certamente agora nossa vida, que devemos viver plenamente, não uma versão fatiada dela" (HIMANEN, 2001, p. 40, tradução nossa).

Segundo Himanen (2001), a ética do trabalho *hacker* está desafiando fortemente a ética Protestante e, de certa forma, está ajudando a mudá-la aos poucos. No entanto, a "ética do dinheiro" não muda. A meta principal de toda forma de capitalismo é acumular dinheiro e, hoje em dia, isso está acontecendo através do "dinheiro virtual" das ações em detrimento do valor do trabalho em si. Na era da economia informacional, as companhias valorizam a ideia de posse e propriedade intelectual e a impressão é que seus prédios parecem prisões de segurança máxima (Ibidem). A tecnologia faz o sistema capitalista se afastar da ética

36 *Skhole* significa "tempo em abundância".
37 Regras de São Bento. XVIII.

protestante. Na economia informacional, a jaula de ferro deixa de ser construída pelos empregados, que colocam o trabalho no topo de suas prioridades, e passa a ser responsabilidade das empresas e patrões que confiam nas pessoas para fazer o trabalho delas, mas não para resguardar suas propriedades intelectuais e posses imateriais.

Há um grande contraste entre essa relação de fechamento que a economia informacional tem com o dinheiro (transformado em ações e propriedades intelectuais) e a abertura que os *hackers* mantêm com o conhecimento. Iniciativas como Linux, distribuído sob a licença *Copyleft*[38], é uma prova que a transmissão de conhecimento e o trabalho feito com paixão ainda são a tônica de tudo que os *hackers* fazem.

Como há uma clara oposição entre o pensamento *hacker* e o capitalismo – algumas vezes eles podem caminhar juntos, como exemplificado anteriormente nos casos dos fundadores da *Sun* e da *Cisco Systems* –, alguns *hackers* propõe uma economia baseada em códigos-abertos. Nela, qualquer pessoa pode modificar os softwares à maneira que for lhes servir melhor, assim como o Linux é hoje. Richard Stallman, líder da Fundação Software Livre, deixa claro que ele não quer proibir ninguém de ganhar dinheiro[39]. A ideia é que não se faça dinheiro guardando a informação para si e sim distribuindo para outros. A proposta dessa nova economia de mercado é ser diferente do capitalismo e do comunismo – ambos regimes político-econômicos regidos pela ética Protestante. A economia do software livre quer disseminar a informação e incentivar a auto-gestão de tempo dos indivíduos.

O Arquivo de Jargões *hacker* fala no tópico sobre a Ética *Hacker* que ela nada mais é do que a crença de que o compartilhamento de informação é um bem positivo e muito poderoso. Compartilhar deve ser, portanto, o dever ético de todo *hacker*. Isso deve ser feito através da criação de códigos abertos e facilitando o acesso aos recursos de informática sempre que possível. Vale pontuar que o tópico no glossário diz que essa ideia não é universalmente aceita[40].

Pekka Himanen (2001) levanta a possibilidade de adaptar a forma de trabalhar dos *hackers* para outras atividades, de forma que o compartilhamento, o ritmo de trabalho individual e a paixão pelo que se faz sejam a tônica da era da informação. Ele propõe que esse pensamento deixe de ser apenas ético e se torne pragmático. Ele usa, mais uma vez, o exemplo da criação do Linux, o mais bem sucedido caso de abertura de pensamento e

38 Licença desenvolvida por Richard Stallman que garante que tudo que é distribuído sob a *Copyleft* seja gratuito e aberto para que outros usuários possa fazer modificações.
39 http://www.gnu.org/philosophy/free-sw.html. Acesso: 17 de novembro de 2013.
40 http://www.catb.org/~esr/jargon/html/H/*hacker*-ethic.html. Acesso: 04 de outubro de 2013.

compartilhamento, que criou um produto estável e confiável não só na comunidade *hacker*, mas para qualquer usuário de computadores.

O modo "código-aberto" de pensar e produzir tem muitas semelhanças com a Ciência e remete, novamente, à Platão, que defendia o alcance da verdade através de diálogos críticos[41]. O modelo de código-aberto, resumidamente, funciona da seguinte forma: alguém estabelece uma meta ou identifica um problema que precisa ser solucionado. Esse alguém normalmente vai propor uma solução (ou apenas apontar aonde ele quer chegar) e dividir isso com a comunidade com a qual ele trabalha – *hacker*, científica, etc. Os outros participantes do processo vão analisar, criticar e fazer novas mudanças, sempre dividindo os resultados com outros e apontando sempre quem fez cada parte do todo. Além dos *hackers* e cientistas, este modelo é utilizado pela Academia.

Há também o "modelo fechado", em que a informação é trancada a sete chaves e somente um grupo selecionado de pessoas pode fazer qualquer tipo de alteração nela. É um modelo autoritário de lidar com o mundo (HIMANEN, 2001). Empresas que prezam a propriedade intelectual e combatem a pirataria utilizam esse modo de pensar e agir. A Microsoft de Bill Gates é uma delas. O modelo fechado é o criado e disseminado pelos mosteiros. "O modelo fechado não permite a iniciativa e a crítica que poderiam tornar uma atividade mais criativa e auto-corretiva" (HIMANEN, 2001, p. 70, tradução nossa).

O modelo aberto de pensamento e produção, compartilhado por *hacker*s, cientistas e acadêmicos, pode parecer confuso e até mesmo anárquico, já que não há uma liderança comandando os processos. No entanto, ele funciona bem organicamente, sem que haja um poder estabelecido que vai ditar os rumos das atividades. Na verdade, há sim algumas pessoas que são espécies de "gurus" ou "mentores". No caso do Linux, é o próprio Linus Torvalds. Ele indica as melhores direções para onde o desenvolvimento do sistema deve seguir e, quando tem duas versões diferentes, deve escolher qual será a oficial. No entanto, caso a referência do grupo não tome a decisão mais acertada, o restante da comunidade vai seguir suas próprias ideias e outra pessoa será eleita o "guru". Não há mandato vitalício.

Há uma tendência nas grandes corporações de aproveitar a tecnologia e seus termos próprios para adaptar seus funcionários e se posicionar no mercado como uma empresa que tem em si o espírito da Era da Informação. Antes, as pessoas eram treinadas em seus trabalhos e desempenhavam essa função todos os dias, até que se aposentassem. Hoje, os trabalhadores são, segundo Castells, "auto-programáveis", e eles têm "a habilidade de se adaptar a novas

41 Praticamente toda a obra de Platão é feita através de diálogos em que Sócrates, seu mentor, é o principal personagem.

tarefas, novos processo e novas fontes de informação, ao passo que a tecnologia, a demanda e o gerenciamento aceleram essa mudança" (CASTELLS, 2000, p. 12). Os funcionários auto-programáveis precisam aprender a lidar com novas rotinas de trabalho, como trabalhar de casa, e estar sempre estudando, porque tudo que ele aprende torna-se obsoleto em pouco tempo. É a cultura do efêmero da qual Castells fala em A Era da Informação. Apesar dessa mudança parecer positiva para o mercado de trabalho e para os próprios trabalhadores, as corporações estão simplesmente adaptando a lógica de computadores a seres humanos para alcançar seu objetivo: ganhar mais dinheiro de forma mais rápida (HIMANEN, 2001).

Além da ética do trabalho *hacker* e da ética do dinheiro, Pekka Himanen aponta em sua obra uma terceira e última regra essencial para os *hacker*s: a "*nethic*[42]", ou ética de rede. A ética de rede é dividida em duas partes: uma que trata da liberdade de expressão nos meios, principalmente na internet, e outra que diz respeito ao direito à privacidade.

As primeiras vozes da ética de rede surgiram em 1990, sob a *Electronic Frontier Foundation*, fundada por Mitch Kapor e John Perry Barlow. A EFF – que teve membros como Steve Wozniak, John Gilmore e Stewart Brand – foi pioneira na luta pela liberdade de expressão e pela privacidade na internet[43]. Os membros da fundação defendiam desde os anos 90 a utilização de encriptação de informação para proteção dos dados das pessoas. Gilmore criou o DES *Crack*er, que era capaz de passar pelo sistema DES utilizada por bancos dos Estados Unidos. "A intenção era demonstrar que os métodos de encriptação permitidos pelos EUA não eram capazes de proteger a privacidade" (HIMANEN, 2001, p. 88, tradução nossa).

Durante os anos 90, a EFF, junto com outras entidades como a XS4ALL e a *Witness*, teve um importante papel na defesa da liberdade de expressão, atuando durante a Guerra do Kosovo, em 1999. O presidente da então Iugoslávia, Slobodan Milosevic, controlava a mídia e censurava aqueles que denunciavam o país pela "limpeza étnica" realizada contra os albaneses. Como a internet é um meio mais difícil de controlar – ao menos naquela época – devido à sua estrutura descentralizada, a EFF, a XS4ALL e a *Witness* atuaram para dar voz ao povo criando um servidor chamado anonymizer.com, que permitia o envio de mensagens que não podiam ser rastreadas, retransmitindo o sinal da rádio B92 – o principal veículo de oposição ao governo e à guerra – via internet quando ela foi fechada pela censura e equipando alguns kosovares para produção de vídeos digitais denunciando o abuso aos direitos humanos. Esses vídeos foram utilizados como prova na Corte Penal Internacional[44]. "Podemos

42 net + ethic.
43 https://www.eff.org/about. Acesso: 05 de outubro de 2013.
44 Witness. Witness Report, 1998-99

considerar a Guerra do Kosovo a primeira guerra em rede, assim como a Guerra do Vietnã foi considerada a primeira guerra televisionada" (HIMANEN, 2001, p. 96, tradução nossa).

Himanen prevê que, no futuro, as pessoas não vão precisar trabalhar em um grande veículo de comunicação para cobrir um evento. Basta ter a mão uma câmera, um telefone e um computador para transmitir em tempo real o que está acontecendo. De fato, estamos vivendo isso atualmente no Brasil, através da Mídia N.I.N.J.A.[45] Provavelmente o autor não estava sendo tão otimista e nem imaginaria que todos esses artefatos estariam reunidos em um só aparelho e nem que a cobertura daria todo o tom – até mesmo fornecendo material e inspirando[46] a mídia tradicional.

Na época em que A Ética *Hacker* e o Espírito da Era da Informação foi escrito, ainda não havia a paranóia por segurança pós-11 de setembro, portanto, Pekka Himanen trata da privacidade apenas para evitar que nossas informações sejam compartilhadas para empresas que vão tentar vender seus produtos para nós ou que nossos chefes possam ter controle sobre o que fazemos em nossas horas de lazer, além de já controlar as horas de trabalho. Isso ainda acontece hoje, mas, principalmente em 2013, a questão da privacidade está ligando-se diretamente ao combate ao terror e ganhou ares de conspiração após a criação do *Wikileaks* e do vazamento de informações da CIA por Edward Snowden. Se Himanen dizia que havia um debate ético nos países desenvolvidos sobre a quebra de sigilo dos cidadãos e que apenas Estados sub-desenvolvidos ou em desenvolvimento controlavam as informações dos indivíduos, ficou claro que qualquer país tem acesso a e-mails, dados de navegação e registros telefônicos de seu povo e que vai acessar esses dados caso interesses estratégicos dependam disso. A única saída para se proteger não só de grandes corporações que têm interesses nas informações das pessoas, mas também dos nossos próprios governos, parece ser a encriptação de e-mails. No entanto, as pessoas que utilizam correspondências superprotegidas, tendem a ser alvo de espionagem justamente por, em teoria, terem algo a esconder. Aparentemente, a melhor forma de ter privacidade é se misturando à massa, vivendo numa alegoria Orwelliana.

> E se construíssemos uma sociedade na qual a informação nunca fosse coletada? Onde você poderia pagar para alugar um filme sem dar seu número do cartão de crédito ou conta no banco? Onde você poderia provar que é apto a dirigir sem ao menos revelar seu nome? Onde você poderia

45 Narrativas Independentes, Jornalismo e Ação.
46 http://www.observatoriodaimprensa.com.br/news/view/_ed763_os_ninjas_da_globonews. Acesso: 05 de outubro de 2013.

> enviar e receber mensagens sem revelar sua localização, como uma caixa de correios eletrônica? Essa é a sociedade que eu quero construir[47].

Podemos entender que toda a ética *hacker* resume-se à criatividade. É necessário ser criativo não só para escrever linhas de código e fazer surgir um sistema operacional ou um programa que será útil para milhões de pessoas, mas também para revolucionar a forma como as pessoas entendem o trabalho, como ganham dinheiro e como distribuem sua obra. De acordo com Himanen, um *hacker* que respeita a ética no que diz respeito ao trabalho, dinheiro e às redes ganha o respeito de toda a comunidade. Um *hacker* que, além disso, é criativo torna-se um herói. Tom Pitman, membro do *Homebrew Computer Club*, compara a criatividade *hacker* com o momento da Criação: "Eu, como cristão, posso dizer que senti algo semelhante à satisfação que Deus deve ter sentido quando ele criou o mundo" (PITMAN, *apud* LEVY, 1984, p. 236, tradução nossa).

47 Tradução nossa para trecho do manifesto Privacy, Techonology, and the Open Society, de John Gilmore em (1991): "*What if we could build a society where the information was never collected? Where you could pay to rent a video without leaving a credit card number or a bank number? Where you could prove you're certified to drive without ever giving your name? Where you could send and receive messages without revealing your physical location, like an electronic post office box? That's the kind of society I want to build.*"

3. CONTEXTO HISTÓRICO

Os ataques terroristas de 11 de setembro de 2001, em Nova York, não mudaram apenas a maior cidade dos Estados Unidos, que perdeu milhares de vidas e seus dois maiores arranha-céus e naquela manhã de terça-feira. O ataque ao World Trade Center e ao Pentágono ficou marcado na História econômica, cultural, política, religiosa e tecnológica do mundo. Os profissionais e entusiastas da Informática já esperavam por grandes mudanças na virada do século, que seriam causadas pelo Bug do Milênio[48]. No entanto, o 11 de setembro trouxe mudanças muito mais drásticas que as imaginadas. Fortes investimentos em sistemas de vigilância em aeroportos, na indústria bélica e, principalmente, na análise de dados deram a tônica da evolução tecnológica dos primeiros anos do século XXI.

3.1. A tecnologia pós-11 de setembro

Após os ataques ao World Trade Center e ao Pentágono as primeiras e maiores mudanças foram feitas na segurança dos aeroportos nos Estados Unidos. Câmeras, *scanners*, revistas invasivas e falta de tolerância com quem não tinha todos os documentos exigidos para viajar aumentaram em todos os terminais de embarque americanos. Os EUA não sofreram mais ataques terroristas em aeroportos ou aviões, mas a segurança excessiva somada ao medo, paranoia e preconceito resultaram em casos como o dos imãs que foram expulsos de um voo da US Airways em 2006 por apresentar "comportamento estranho", como rezar no portão de embarque[49]. A perseguição aos árabes e muçulmanos se tornou comum e foi incentivada pelo Departamento de Segurança Interna dos Estados Unidos, que recomendava aos americanos "reportar qualquer suspeita de atividade criminosa ou terrorista ao FBI"[50].

Outra mudança fundamental pós-11 de setembro foi vista nas grandes corporações e nas formas como elas armazenam seus dados e protegem sua infraestrutura e seu pessoal. A

48 Problema que seria causado na virada do ano 1999 para 2000 e afetaria todas as datas com sistemas informatizados. O bug seria um erro de lógica causado pela economia de bytes na programação, escrevendo os anos com apenas dois dígitos em vez de quatro. Assim, os computadores poderiam entender que à meia-noite do dia 1º de janeiro estaríamos entrando no ano 1900 e não 2000. Isso causou um pânico coletivo devido aos boatos de que esse problema resultaria em quebras de bolsas de valores, falhas letais em usinas nucleares, acidentes áereos, etc. Na virada do ano, nada aconteceu.

49 http://www.nytimes.com/2006/11/22/us/22muslim.html. Acesso: 28 de outubro de 2013.

50 http://web.archive.org/web/20061024191815/http://www.dhs.gov/xinfoshare/reportincidents. Acesso: 28 de outubro de 2013. Hoje a página não existe mais devido à discriminação exagerada que tomou conta da população norte-americana. O Departamento de Justiça dos EUA trabalha para garantir a não-violação dos direitos civis de árabes, muçulmanos, sikhs e americanos com ascendência da Ásia Meridional (http://www.justice.gov/crt/legalinfo/nordwg_mission.php).

jornalista Sherri Welch, do jornal Crains Detroit Business, reaviva a questão da ética Protestante em relação ao trabalho. "A visão de segurança deixou de se preocupar em manter as pessoas fora do escritório em suas horas livres para ter ciência de tudo que elas estão fazendo nas horas de trabalho"[51].

As empresas passaram a se preocupar muito mais com seus dados, principalmente as que mantinham informações confidenciais e servidores no World Trade Center. Uma saída encontrada por elas foi manter cópias desses servidores e arquivos em mais de um local do país para evitar que seus dados se perdessem caso um novo ataque terrorista venha a acontecer. No entanto, a criação do USA Patriot Act[52] em 26 de outubro de 2001 não garantia mais a segurança de dados e informações confidenciais das empresas. Muitos investidores estrangeiros e multinacionais preferiram alocar seus arquivos fora do país para se proteger de possíveis espionagens e quebras de sigilo por parte do governo americano.

O Patriot Act foi o ponto de partida para o início dos grandes projetos de espionagem do FBI e da CIA, como o PRISM, e culminaram nas recentes denúncias de Edward Snowden sobre os milhões de cidadãos que estavam tendo suas caixas de e-mail e registros telefônicos vigiados permanentemente, sob a alegação de que o governo estaria buscando informações para evitar futuros ataques terroristas. Boa parte dessa espionagem é feita eletronicamente por *hacker*s que trabalham para o governo. A virada do século foi marcante para os *hacker*s porque os Estados Unidos passaram a valorizar muito os programadores, seja para trabalhar nas milhões de empresas de internet que surgiram na última década, seja para auxiliar na Guerra ao Terror praticando espionagem eletrônica, quebra de sigilo de suspeitos ou criando programas que auxiliam as Forças Armadas. Algumas iniciativas surgiram para criar uma nova geração de americanos que saibam programar e aprendam linhas e códigos desde a escola, como se fosse o alfabeto. O code.org é uma dessas iniciativas, apoiada por Bill Gates, Al Gore, Mark Zuckerberg, e celebridades do mundo da música e do esporte. O code.org quer que todos os estudantes dos EUA tenham acesso a aulas de ciência da computação, além de fazer com que mais mulheres e negros tornem-se nomes de referência na área[53]. Outra

51 http://www.crainsdetroit.com/article/20110911/FREE/309049965/9-11-forced-big-changes-for-biz-increased-security-often-costly#. Acesso: 29 de outubro de 2013.

52 Acrônimo para Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001 (em tradução livre Ato de 2001 para unir e fortalecer a América providenciado as ferramentas adequadas necessárias para interceptar e obstruir o terrorismo). O Patriot Act permite a detenção por tempo indefinido de imigrantes, a realização de buscas em propriedades privadas sem a autorização dos proprietários e o acesso a e-mails, registros telefônicos e bancários sem ordem judicial. Em 26 de maio de 2011, Barack Obama estendeu por mais quatro anos algumas atividades do Patriot Act: http://articles.latimes.com/2011/may/27/nation/la-na-patriot-act-20110527. Acesso: 29 de outubro de 2013.

53 http://code.org/about. Acesso: 17 de novembro de 2013.

fundação é o *Codeacademy*, site que oferece aulas de programação online para interessados em aprender diversas linguagens ou aperfeiçoar seus conhecimentos. Além das aulas gratuitas, o Codeacademy permite que pessoas criem cursos e os disponibilizem sem custos na plataforma do site[54].

A vigilância fez com que muito dinheiro fosse investido em tecnologia para melhorar os resultados da chamada "mineração de dados", que é o vasculhamento de grandes quantidades de dados em redes sociais e e-mails. A mineração de dados é a análise de informações feita de forma detalhada, para localizar os motivos que possam ter levado uma pessoa a comprar determinado produto, ao envio de um *e-mail* ou ao acesso a algum *site*. É como ampliar uma fotografia ao máximo para enxergar seus detalhes, ao contrário do *big data* – do qual falarei adiante –, onde a imagem é vista de longe para tentar ver o cenário e o contexto onde ela se encontra[55]. De acordo com Rohini Srihari, pesquisadora da State *University of New York* e fundadora da *Janya* – empresa de mineração de dados já extinta –, o desafio que se tem nesse ramo é a análise do conteúdo para entender jargões e códigos e também ter acesso a informações que não são públicas, já que "as pessoas que fazem um 11 de setembro não falam sobre o assunto no *Twitter*"[56].

3.2. O B*ig Data* como arma econômica e de guerra

O *Big Data* é a armazenagem de grande quantidade de dados, normalmente na ordem de Petabytes[57], e com alto grau de complexidade para ser analisado por computadores e *softwares* comuns[58]. O termo foi criado por Doug Laney, analista da empresa de consultoria Gartner, em 2001. Laney afirmou que o constante crescimento de informação e dados traria três grandes desafios para a indústria da tecnologia da informação. Esses desafios foram colocados no modelo dos "3Vs", que são o volume (quantidade de dados), velocidade (na entrada e saída de dados) e variedade (de tipos e fontes de dados)[59]. Algumas correntes adicionam um quarto "V" ao modelo que define o *Big Data*, o V de veracidade. Segundo esse

54 http://www.codecademy.com/pt/about. Acesso: 17 de novembro de 2013.
55 http://www.slideshare.net/PeterCochrane/big-data-v-data-mining. Acesso: 29 de outubro de 2013.
56 http://www.technologyreview.com/article/425380/what-has-technology-fixed-since-911. Acesso: 29 de outubro de 2013.
57 Um Petabyte equivale a um quatrilhão de bytes.
58 http://mike2.openmethodology.org/wiki/Big_Data_Definition. Acesso: 30 de outubro de 2013.
59 http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf. Acesso: 31 de outubro de 2013.

pensamento, a veracidade é importante para confiar na integridade dos dados para que eles sejam usados em decisões estratégicas e confidenciais[60].

Como mostra a definição do que é o *Big Data* do site MIKE 2.0 (ver referência 53), nem sempre os dados são "*big*" do ponto de vista da armazenagem e sim do ponto de vista da complexidade de análise. Em um voo de cerca de uma hora, por exemplo, um avião gera informações muito complexas sobre condições climáticas, utilização do combustível, controles que foram acionados, momentos de turbulência, altura em que o avião se encontra e muito mais. No entanto, esses dados podem ser armazenados em um simples *pendrive* de uso pessoal, já que dificilmente eles vão ocupar mais que três gigabytes.

O *Big Data* se tornou popular em 2008, quando foi tema de um artigo escrito por Chris Anderson na conceituada revista *Wired* – este artigo será debatido mais a frente – e foi abraçado por um grupo de cientistas americanos do *Computing Community Consortium* (CCC), fundação que reúne pesquisadores acadêmicos e corporativos da *National Science Foundation* e *Computing Research Association*[61]. Ainda em 2008, a gigante IBM adotou o *Big Data* como ferramenta de marketing e dedicou páginas em seu portal e redes sociais ao assunto, onde são encontrados estudos de caso de empresas que fizeram uso bem sucedido da análise da grande quantidade de dados, notícias e novas pesquisas sobre o assunto. Em 2011, a IBM, em um grande trabalhado que utilizou *Big Data* e inteligência artificial, criou um robô que venceu o popular programa de perguntas e respostas norte-americano Jeopardy[62]. A façanha conquistada pelo robô Watson e o prêmio de 1 milhão de dólares colocaram o *Big Data* de vez sob os holofotes do mundo da tecnologia.

O jornalista Steve Loht, do New York Times, lembra que a análise de dados é uma atividade que existe no mundo há, no mínimo, dois séculos, e a tendência é que a quantidade de informação seja sempre crescente.

> Pilhas crescentes de dados têm sido um desafio há tempos. No final do século 19, os recenseadores fizeram um grande esforço para contar e categorizar o crescimento acelerado da população dos Estados Unidos. Um avanço inovador chegou a tempo para o censo de 1890, quando a população alcançou a marca de 63 milhões de pessoas. A ferramenta de aferição de dados perfeita para o momento foi cartão perfurado inventado

60 http://www.villanovau.com/university-online-programs/what-is-big-data. Acesso: 31 de outubro de 2013.
61 O CCC publicou um guia básico sobre o *Big Data* explicando seu funcionamento, como pode ser utilizado e como ele vai influenciar o mundo no século XXI. "Big Data Computing: Creating revolutionary breakthroughs in commerce, science, and society" pode ser acessado em http://www.cra.org/ccc/files/docs/init/Big_Data.pdf.
62 http://www.nytimes.com/2011/02/17/science/17jeopardy-watson.html. Acesso: 01 de novembro de 2013.

> por Herman Hollerith. Estes cartões foram o alicerce tecnológico da companhia que viria a se tornar a IBM[63].

A grande vantagem do *Big Data* em relação a outras tecnologias de análise de dados foi o marketing feito em cima dele. Seu nome e conceito chamam atenção, a ideia de um grande volume de dados que não podem ser armazenados e analisados por qualquer computador e *software* criam uma mística de que o *Big Data* é a mais poderosa fonte de informação disponível atualmente. De fato, o nome que remete ao *Big Brother* e a quantidade de informações coletadas por empresas como o *Google* e o *Facebook* fazem dele uma poderosa e quase inesgotável fonte com informações sobre padrões de consumo. De acordo com um estudo realizado pela consultoria *McKinsey & Company* em 2011, o *Big Data* será fundamental para o crescimento e competitividade de empresas. Ele vai permitir o mapeamento de como os clientes se comportam e oferecer informações do que eles precisam, permitindo às corporações criar novos produtos "customizados" pelas preferências dos consumidores e também traçar suas estratégias de mercado, além de permitir a coleta e armazenamento quase infinito de informações detalhadas[64]. Hoje, o *Google* o *Facebook* podem ser considerados os grandes expoentes do *Big Data* para o mundo, já que nós somos impactados diretamente por suas análises de informações, que chegam através de anúncios personalizados em caixas de e-mail e perfis pessoais nas redes sociais. Tudo é baseado nos comportamentos que temos online, traçado através das buscas que realizamos, da utilização de termos chaves em nossas mensagens particulares e nos conteúdos que acessamos.

Assim como *data mining* foi utilizado para buscar terroristas e evitar novos ataques, cada vez mais o *Big Data* está tomando espaço na guerra ao terror. Se antes os militares e o serviço secreto norte-americano buscavam encontrar mensagens nas entrelinhas e entender as motivações dos terroristas, hoje, com o *Big Data*, faz-se um distanciamento do cenário para identificar os nós que formam a rede que poderia resultar em novo 11 de setembro.

O *Big Data* usado como arma de guerra provem de uma mentalidade segundo a qual remediar é melhor que prevenir. Com o *Big Data*, faz-se a análise de muito mais dados e em velocidade extremamente superior a que era feita há alguns anos. É possível identificar comportamentos suspeitos mesmo que eles estejam fortemente codificados (o que também leva a erros de julgamento, mas isto será tratado a fundo mais adiante) e desmantelar células

63 http://www.nytimes.com/2012/08/12/business/how-big-data-became-so-big-unboxed.html. Acesso: 01 de novembro de 2013.
64 http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation. Acesso: 01 de novembro de 2013.

terroristas no início da execução de um plano de ataque. No entanto, não há preocupação em investigar porque terroristas tornam-se terroristas, como eles conseguem entrar no território norte-americano, como têm acesso à armas ou quais são as motivações que podem levar um cidadão dos Estados Unidos a entrar para um grupo terrorista. O pesquisador e cientista político Evgeny Morozov alerta para o perigo de não se preocupar em encontrar as reais motivações do terrorismo e focar somente em soluções paliativas:

> A grande tentação do Big Data é que nós podemos parar de nos preocuparmos com a compreensão. Em vez de gastar recursos públicos preciosos tentando entender o "porquê", podemos focar em prever o "quando", então uma intervenção pontual será feita. […] Como um curativo, o *Big Data* é excelente. Mas curativos são inúteis quando o paciente precisa de uma cirurgia. Nesse caso, usar um curativo pode causar uma amputação.[65]

Chris Anderson, autor do livro Cauda Longa e editor da Wired, escreveu em um artigo em 2008, ano da "grande virada" do *Big Data*, sobre o fim da teoria científica[66]. Ele diz que empresas como o *Google* são as "crianças dos *Petabytes*" e não se importam com análises causais e semânticas, apenas com a matemática que dá resultados. Anderson utiliza o exemplo do *ranking* do *Google* para definir quais páginas aparecem primeiro quando realizamos uma busca. Em teoria, as primeiras páginas são as "melhores" sobre o assunto pelo qual pesquisamos, mas não sabemos por que o conteúdo delas são melhores e mais relevantes. Elas só aparecem nas primeiras posições por causa dos algoritmos que identificam as boas práticas de SEO das páginas[67].

> Este é um mundo onde uma quantidade massiva de dados e matemática aplicada substituem qualquer outra ferramenta que possam apontar. É o fim de qualquer teoria do comportamento humano, de linguística à sociologia. Esqueça a taxonomia, ontologia e psicologia. Quem sabe por que as pessoas fazem o que elas fazem? A questão é que elas fazem, e nós podemos traçar e medir isso com uma exatidão sem precedentes. Com a quantidade suficiente de dados, os números falam por si.[68]

---

65 http://www.slate.com/articles/technology/future_tense/2013/06/with_big_data_surveillance_the_government_doesn_t_need_to_know_why_anymore.html. Acesso: 01 de novembro de 2013. Tradução nossa.

66 http://www.wired.com/science/discoveries/magazine/16-07/pb_theory. Acesso: 02 de novembro de 2013.

67 *Search Engine Optimization* (Otimização para mecanismos de pesquisa). É um conjunto de técnicas e estratégias que fazem com que determinado site se torne mais relevante em uma busca orgânica, gerando mais acessos, conversões e vendas.

68 http://www.wired.com/science/discoveries/magazine/16-07/pb_theory. Acesso: 02 de novembro de 2013. Tradução nossa

Para Anderson, a utilização do *Big Data* vai tornar o método científico obsoleto porque o estudo da causalidade e das conexões que confirmam uma hipótese será deixado de lado. A análise de dados, em conjunto com a matemática, fará com que as correlações sejam suficientes para que possamos determinar verdades científicas sem nos preocuparmos com a possibilidade de ser apenas uma coincidência. Essa mudança de paradigma atinge o ponto central da Ética *Hacker* de Pekka Himanem. Para ele, o *modus operandi* dos *hacker*s se assemelha aos métodos acadêmico e científico, uma vez que eles analisam as hipóteses antes de criar ou alterar uma linguagem de programação.

A tendência é que cada vez mais a guerra ao terror promovida pelo governo norte-americano seja feita de forma virtual e com auxílio do Big Data. Nos últimos dois anos foram investidos mais de 10 bilhões de dólares e a previsão de investimento para 2014 na tecnologia é de 6 bilhões[69].

69http://www.biometricupdate.com/201308/u-s-government-spending-on-big-data-to-grow-exponentially. Acesso: 04 de novembro de 2013.

4. *WIKILEAKS* – OS *HACKERS* DO JORNALISMO

O *WikiLeaks* é uma organização de mídia transnacional sem fins lucrativos. O site, que tem sede na Suécia, publica em suas páginas documentos, informações confidenciais, vídeos, áudios e outros materiais sensíveis para o interesse de governos ou grandes empresas. Utilizando uma tecnologia que protege suas fontes e permite que o envio desses dados seja feito de forma online e segura, o *WikiLeaks* tem como missão fornecer material jornalístico sem ter que se submeter a interesses políticos e econômicos, denunciando escândalos e mostrando a verdade para quem quiser vê-la sem omissão de qualquer informação. Além de fazer relatos jornalísticos, o site também permite que qualquer um tenha acesso aos documentos que pautam suas matérias, sendo também fonte para outros meios de comunicação.

O *WikiLeaks* foi criado em 2006 e seu principal representante é o australiano Julian Assange, jornalista e ciberativista. Assange estudou matemática e física e foi um *hacker* antes de ajudar a fundar o WikiLeaks e se tornar o porta-voz oficial da organização. Ele está refugiado na embaixada do Equador em Londres desde junho de 2012[70], quando pediu abrigo após o Reino Unido anunciar sua extradição para a Suécia, onde é acusado de estupro e abuso sexual. Julian Assange também é procurado pela Interpol e pode responder pelos crimes de espionagem, conspiração e tráfico de informações confidenciais nos Estados Unidos[71].

Entre os principais vazamentos do *WikiLeaks* estão o manual de tratamento aos presos dos campos militares dos Estados Unidos, como Guantanamo e outros no Iraque[72], documentos que reportavam a morte de milhares de civis causadas pelos americanos na Guerra do Afeganistão e o vídeo de um helicóptero Apache do exército dos EUA atacando insurgentes em Bagdá durante a ocupação do Iraque, em 2007. O material causou grande revolta da opinião pública e de parte da imprensa que criticava a guerra. Este vídeo é, talvez, a mais importante publicação que o *site* já fez e mostra a morte de 12 pessoas, entre elas dois jornalistas iraquianos que trabalhavam para a agência de notícias Reuters, além de homens desarmados e duas crianças feridas. O vídeo do ataque aéreo em Bagdá tornou-se emblemático para o *WikiLeaks* porque a fonte que forneceu o material para o site foi revelada

70 http://abcnews.go.com/Blotter/ecuador-grants-wikileaks-founder-assange-political-asylum/story?id=17018133. Acesso: 13 de novembro de 2013.
71 http://www.nytimes.com/2010/12/08/world/08leak.html. Acesso: 13 de novembro de 2013.
72 http://wikileaks.org/detaineepolicies. Acesso: 13 de novembro de 2013.

e condenada por violação do Ato de Espionagem de 1917[73]. Chelsea Manning (conhecida como Bradley Manning antes de iniciar o tratamento de terapia hormonal para mudança de sexo[74]) é uma soldado do exército norte-americano que foi Analista de Inteligência no Iraque. Com seu acesso a informações confidenciais das forças armadas, ela divulgou o vídeo do ataque aéreo em Bagdá, além de relatórios de guerra do Iraque e do Afeganistão. Há um debate sobre a linha tênue sobre o que é traição e espionagem e o que é jornalismo. Para Julian Assange, condenar Chelsea Manning pela divulgação dos horrores da guerra é abrir um precedente que pode levar à extinção do jornalismo investigativo[75]. Por outro lado, a corte marcial dos Estados Unidos afirma que os documentos e o vídeo que foram vazados por ela facilitam o trabalho de organizações terroristas e governos inimigos dos EUA, que podem ter acesso facilmente a essas informações.

Pode-se pensar que o *WikiLeaks* nada tem a ver com *hackers*, por ser essencialmente uma organização de mídia e, por mais que não esteja atrelada a corporações, governos e outras instituições que possam influenciar seu trabalho, é mais um veículo jornalístico. No entanto, analisando as atividades do site, a tecnologia utilizada e os valores de seus criadores, podemos estabelecer diversas conexões com a cultura *hacker* e, principalmente, a ética *hacker*. Se Pekka Himanen falou do espírito da era da informação, o *WikiLeaks* pode ser considerado um dos grandes expoentes da ética *hacker* na era do sigilo da informação.

O jornalista Pablo Mancini fala em seu livro "Hackear el Periodismo" que o jornalismo precisa ser *hackeado* para sobreviver às novas tecnologias que permitem ao público ser não só consumidor de notícias, mas também produtor das informações. Hoje, qualquer um possui as ferramentas necessárias para apurar, escrever, filmar, gravar e disseminar um fato. Ainda que um indivíduo não conte com todo o aporte que um grande veículo de comunicação possui, ele pode facilmente fazer com que sua versão dos fatos seja vista por milhares – podendo chegar a milhões – de pessoas e estabelecer um contraponto a grande mídia. A questão principal do livro é entender como o jornalismo pode utilizar o pensamento *hacker* para oferecer conteúdo de qualidade ao público e manter seu valor

73 O Ato de Espionagem é uma lei criada após a Primeira Guerra Mundial que proíbe interferências em operações militares, apoio aos inimigos dos Estados Unidos em tempos de guerra, insubordinação militar ou interferência no recrutamento das Forças Armadas. Desde sua criação, em 15 de junho de 1917, já teve diversas emendas adicionadas ao texto original. O texto original pode ser acessado em http://www.law.cornell.edu/uscode/text/18/part-I/chapter-37

74 http://www.today.com/news/i-am-chelsea-read-mannings-full-statement-6C10974052. Acesso: 13 de novembro de 2013.

75 http://info.abril.com.br/noticias/seguranca/2013/07/culpar-manning-de-ajuda-ao-inimigo-destroi-jornalismo-investigativo-diz-assange.shtml. Acesso: 13 de novembro de 2013.

comercial. Para "salvar" o jornalismo, Mancini (2011) propõe quatro pontos fundamentais para entender o processo e permitir o *hack* nas redações: tempo, público, valor e organização.

O desafio do tempo é preencher o *in-between time* do público, infiltrando-se em sua hiperconectividade, já que o *prime time* está saturado[76]. A relação que o "jornalista *hacker*" deve ter com o público é estabelecida a partir do momento em que ele entende que os meios não são os detentores exclusivos das ferramentas de produção e distribuição de conteúdo, deve-se pensar em como abordar e verdadeiramente entrar em contato com as pessoas. O valor é criado através de meios programáveis e com uma gestão eficiente para as conversações, já que muito do valor dos conteúdos hoje em dia vêm do público, que remixa e faz pós-produções daquilo que os agrada. Por último, vem a organização, que deve ser alcançada por experimentações organizacionais para buscar a melhor forma possível neste novo jornalismo.

O WikiLeaks se vale muito das questões do valor e da organização. O valor é alcançado através da utilização de informações que chegam a eles por fontes anônimas que podem enviar material através do site, de forma criptografada[77] e sob as leis de sigilo de imprensa da Suécia e da Bélgica. O site também permite o envio postal de material. A indicação que eles dão é que seja enviada mais de uma cópia do arquivo, por serviços postais diferentes, e que os CDs, DVDs e/ou USBs sejam criptografados, comprados em dinheiro e enviados de locais distantes da residência da fonte que está enviando o material. A extrema preservação das fontes do site e a possibilidade de criptografar os conteúdos fornecidos por elas estabelecem uma relação fonte-veículo pouco vista no jornalismo, já que os meios tradicionais não preservam seus informantes após conseguirem os dados que precisam para a matéria. O material do *WikiLeaks* possui grande valor porque é oriundo de um público que tem acesso a informações confidenciais e secretas de governos e empresas. Ao publicar os relatos no site e disponibilizar os arquivos originais, também permite ao grande público ver uma informação jornalística sem edições e que serve de pauta para outros meios de comunicação, que gastariam muito tempo e sofreriam muitos riscos se tivesse que apurar tais informações. Os *publishers* tradicionais se tornam amplificadores de um conteúdo gerado fora das redações tradicionais.

76 O *prime time* do jornalismo é o horário nobre da televisão e o momento de leitura do jornal pela manhã. O *in-between time* são os momentos de descanso e pequenos intervalos que o público tem durante o dia, como horário de almoço e durante os deslocamentos para o trabalho e de volta para casa onde acessam informação via celulares e tablets.

77 Tecnologia que torna a informação ilegível, de forma que somente o receptor que tem a chave decodificadora pode ter acesso a mensagem original. Isso evita que os dados sejam acessados por pessoas não autorizadas.

A organização do *WikiLeaks* é extremamente importante para a manutenção do site, que sofre diversos ataques DDoS[78] sempre que divulga informações extremamente confidenciais e sensíveis. A primeira vez que isso aconteceu foi em novembro de 2010, logo após o vazamento dos telegramas diplomáticos dos Estados Unidos[79]. O Brasil é assunto de alguns dos 250 mil telegramas diplomáticos dos Estados Unidos vazados pelo WikiLeaks. Os documentos mostravam que as embaixadas norte-americanas no país se preocupavam com possíveis terroristas vivendo no Brasil, locais do país que pudessem ser alvos de ataques e as relações do governo brasileiro com Venezuela e Irã. As ações da presidenta Dilma Roussef durante a ditadura e os programas do PT como o Fome Zero e o Bolsa Família também foram alvo das conversas entre os diplomatas[80].

Além dos ataques aos servidores e da pressão política, o WikiLeaks sofreu boicotes de empresas como o Tableau Reports – que removeu a visualização de dados e gráficos sobre os acessos aos telegramas diplomáticos –, PayPal, Visa e MasterCard – que suspenderam a utilização de seus serviços para doações ao site – e a Amazon e a everyDNS.com, que pararam de oferecer seus servidores e roteadores ao WikiLeaks sob a alegação de que os ataques DdoS estavam prejudicando seus outros serviços e clientes. Assim, o endereço wikileaks.org saiu do ar em dezembro de 2010 e voltou a funcionar sob o domínio wikileaks.ch, que é registrado na Suíça, mas fica na Suécia. Hoje, o WikiLeaks possui vários "sites espelho"[81] que replicam o conteúdo do site original e que continuam ativos mesmo sem o servidor principal. Como esses espelhos ficam hospedados em diversos sites, cada um possui uma regulamentação diferente de internet e no que diz respeito a vazamento de informações confidenciais e espionagem. Portanto, mesmo que um espelho ou o site principal seja retirado do ar, os outros endereços continuarão ativos e acessíveis para qualquer pessoa.

A organização do WikiLeaks se assemelha à metáfora do bazar, proposta por Eric Raymond no livro "A Catedral e o Bazar". Ao se espalhar por diversos domínios e não depender somente de um endereço principal, o WikiLeaks se mostra totalmente mutável e permite que qualquer pessoa espelhe seu conteúdo sem restrições. O WikiLeaks é como um bazar que se muda de local e se remodela e não a uma catedral, que é imutável e que, uma vez

78 *Distributed Denial of Service*, Ataque Distribuído de Negação de Serviço. É uma tentativar de derrubar servidores, tornando-os inativos para seus utilizadores. O ataque distribuído é feito a partir de um computador mestre, que controla diversas máquinas "zumbis" e as faz acessar determinado conteúdo, sobrecarregando os servidores e inutilizando seus serviços. Acredita-se que o governo norte-americano tenha sido o responsável pelos ataques que o WikiLeaks sofreu.

79 http://www.theguardian.com/media/2010/dec/07/wikileaks-under-attack-definitive-timeline. Acesso: 15 de novembro de 2013.

80 http://wikileaks.org/tag/BR_0.html. Acesso: 17 de novembro de 2013.

81 Lista dos sites espelho do WikiLeaks: http://wikileaks.info. Acesso: 15 de novembro de 2013.

construída, não pode se mudar. Mesmo que seja reformada, sua fundação continua sendo a mesma (RAYMOND, *apud* MANCINI, 2011).

Além dos espelhos, no dia 16 de agosto de 2013, o WikiLeaks disponibilizou arquivos criptografados que, somados, têm mais de 400gb e solicitou que as pessoas baixassem esses arquivos e replicassem pela internet[82]. Não se sabe qual tipo de conteúdo está disponível nestes arquivos, mas existem duas fortes especulações do que podem ser: todas as informações sobre o esquema de espionagem da Agência de Segurança Nacional dos Estados Unidos revelado por Edward Snowden ou as identidades de todos os agentes secretos norte-americanos que estão na ativa, com informações sobre seus trabalhos e onde eles atuam[83]. Por estar criptografado, os conteúdos dos arquivos são inacessíveis. Acredita-se que o *WikiLeaks* está praticando chantagem com o governo norte-americano ao não revelar o que estes arquivos contêm e nem liberando a chave de acesso, criando um temor de que eles possuem informações muito mais relevantes e confidenciais do que todas as outras já divulgadas pelo site. Também há a teoria de que tudo não passe de um blefe, já que o *WikiLeaks* nunca escondeu nenhuma informação confidencial sobre governos e o arquivo pode ser somente um *backup* do site para que ele seja recolocado no ar caso volte a ser derrubado e os espelhos também saiam do ar. A criação de um arquivo altamente criptografado é mais uma prova que o WikiLeaks não existiria sem os *hackers*. Este nível de criptografia só é feito por pessoas com sólidos conhecimentos de programação e segurança da informação.

Os princípios da Ética *Hacker* escritos por Steven Levy de que toda informação deve ser livre e que o acesso à coisas que ajudem a entender como o mundo funciona deve ser ilimitado se aplicam perfeitamente ao *WikiLeaks*. A proposta do site de "vazar" informações é uma forma de combater injustiças, permitindo que qualquer um saiba o que realmente acontece na guerra e como grandes negócios são fechados. Julian Assange disse em 2006, pouco depois da fundação do *WikiLeaks*, que "somente injustiças que são reveladas podem receber uma resposta. Para que qualquer atitude inteligente seja tomada, é preciso saber o que está acontecendo"[84].

A proposta do *WikiLeaks* de que toda informação deve ser livre levanta um debate acerca de dados privados de usuários de serviços como o *Google* e o *Facebook*. Se telegramas diplomáticos merecem ser vistos e compartilhados por qualquer pessoa, por que não as

82 https://www.facebook.com/wikileaks/posts/561927090509074. Acesso: 15 de novembro de 2013.
83 http://www.dailydot.com/politics/wikileaks-insurance-file-facebook-encrypted. Acesso: 15 de novembro de 2013.
84http://www.spiegel.de/netzwelt/netzpolitik/wikileaks-maechtige-spueren-die-macht-der-*hacker*-ethik-a-732785.html . Acesso: 15 de novembro de 2013.

informações pessoais que fornecemos aos sites que visitamos? Nossas mensagens de e-mail, compras realizadas online e endereços devem ser disponibilizados para que qualquer pessoa – ou corporação – no mundo possa vê-los? Wau Holland, fundador do *Chaos Computer Club*[85], adicionou mais dois princípios da Ética *Hacker* além dos que foram propostos por Steven Levy. Uma delas é que não se deve mexer nos dados de outro *hacker* e, uma que faz todo sentido nos dias atuais, é a que diz que se deve disponibilizar dados públicos, ao mesmo tempo em que deve-se proteger os dados privados[86].

85 Fundado em 1981, o *Chaos Computer Club* é uma associação alemã de *hacker*s e a maior da Europa. O CCC luta por livre acesso à informação, mais transparência de governo e direito à comunicação. Para maiores informações, acesse http://www.ccc.de/en.

86http://www.spiegel.de/netzwelt/netzpolitik/wikileaks-maechtige-spueren-die-macht-der-*hacker*-ethik-a-732785.html. Acesso: 17 de novembro de 2013.

5. A RELAÇÃO ENTRE *HACKERS* E GOVERNO

Apesar da Cultura *Hacker* ter nascido no ambiente acadêmico e utilizado tecnologias criadas por militares para se desenvolver e se espalhar pelo mundo, os *hackers* nunca tiveram uma relação amistosa com governos e poderes estabelecidos. No entanto, acontecimentos da última década, como o 11 de setembro e o desenvolvimento exponencial da tecnologia e seu avanço como ferramenta fundamental no dia a dia da sociedade ocidental, estão mudando esse panorama.

Assim como a ética do trabalho sofreu mudanças em pontos chave da História, como a reforma protestante e o surgimento do capitalismo, os ataques terroristas ao *World Trade Center* e ao Pentágono iniciaram uma nova era no que diz respeito ao trabalho. A guerra ao terrorismo cada vez mais depende da tecnologia e hoje em dia é possível até mesmo impedir os planos de uma nação inimiga utilizando vírus de computador[87]. Esta guerra cibernética que vem se construindo nos últimos anos precisa de contingente preparado para os campos de batalha virtuais, justamente por isso o governo norte-americano vem recrutando *hacker*s nos últimos anos para suprir a demanda das agências de segurança por pessoas qualificadas na arte da programação e da invasão de sistemas de segurança.

O primeiro passo público dos Estados Unidos na sua busca por "*hackers* éticos" (este é o termo utilizado pelas agências americanas e será explicado mais a frente) começou em 2009, quando o próprio governo admitiu estar preparado para ataques aéreos, explosões, enchentes ou incêndios, mas que não saberia como agir caso sofresse um grande ataque cibernético[88].

Em agosto de 2011, agentes federais norte-americanos do Departamento de Defesa, Departamento de Segurança Interna e da Agência de Segurança Nacional participaram de um painel na DEFCON, a maior conferência de *hackers* do mundo, chamado "*Meet the Feds*"[89]. De acordo com a matéria do *Huffington Post*, o "encontro com os federais" tinha como objetivo recrutar pessoas para trabalhar para o governo na prevenção a ataques e espionagem

87 http://www.theguardian.com/technology/2013/feb/26/symantec-us-computer-virus-iran-nuclear. Acesso: 20 de novembro de 2013. O *Stuxnet* é um vírus criado para infectar o sistema operacional SCADA, que controla as centrífugas de enriquecimento de urânio do Irã e foi criado pela Siemens. Acredita-se que o vírus tenha sido criado pelos Estados Unidos e Israel, mas os países nunca confirmaram a autoria. O Stuxnet contaminou os computadores da Estação Espacial Internacional com um pendrive que carregava o vírus. Mais detalhes em: http://www.ibtimes.co.uk/articles/521246/20131111/international-space-station-infected-malware-russian-astronaut.htm.

88 http://phys.org/news159342320.html. Acesso: 20 de novembro de 2013.

89 http://www.huffingtonpost.com/2011/08/08/government-recruits-*hacker*s-cyber-shortage_n_920795.html. Acesso: 20 de novembro de 2013.

cibernética. À época, os EUA precisavam de 10 a 30 mil especialistas na área. Em 2008 havia apenas um número em torno de mil *hackers* trabalhando nas instituições federais.

A princípio, o motivo de estar em busca de *hackers* para as agências federais era acompanhar a Rússia e a China, países que criaram programas de desenvolvimento de *hackers* e estavam muito a frente dos EUA. Os russos lançaram seu programa de treinamento de cibersegurança em 1995, quando a internet ainda estava se popularizando. O governo chinês promove competições de *hackers.* Um dos vencedores dessas disputas foi pego invadindo sistemas federais norte-americanos[90].

Em março de 2007, o Pentágono anunciou sua estratégia oficial de segurança cibernética após ter mais de 24 mil documentos roubados por *hacker*s estrangeiros[91]. Assim, a posição do Departamento de Defesa dos Estados Unidos foi se mostrar como vítima de ataques cibernéticos e adotar uma postura de defesa e segurança na rede, além de fazer parcerias com as nações aliadas[92]. Os EUA nunca se mostraram oficialmente a favor de uma guerra cibernética baseada em espionagem, ataque de sistemas e servidores, mas dominar o espaço virtual através da ocupação tecnológica, assim como faz com as forças armadas tradicionais. Recentes revelações de que a NSA (Agência Segurança Nacional) espiona diversas nações e empresas mostram que, mesmo no ciberespaço, a estratégia dos Estados Unidos tende a ser ofensiva.

Ainda é estranho para *hackers* de formação, que desenvolveram suas habilidades sob os ensinamentos de nomes como Richard Stallman e Linus Torvalds, trabalharem para o governo e, mais do que isso, colocarem-se contra outros *hackers* numa espécie de batalha naval virtual[93]. Fazer com que dados governamentais de interesse público permaneçam secretos e se colocar numa posição de embate com outro *hacker* apenas por ele pertencer a uma nação diferente vai contra dois pontos essenciais da ética *hacker* proposta por Steven Levy. Por isso, iniciativas como o code.org, citado anteriormente, são essenciais para o desenvolvimento de novos *hacker*s que não sejam "ideologicamente contaminados" e que sejam *hackers* apenas no que diz respeito aos conhecimentos técnicos.

---

90 http://www.huffingtonpost.com/2013/01/28/pentagon-cyber-force_n_2567564.html. Acesso: 20 de novembro de 2013.

91 http://www.huffingtonpost.com/2011/07/14/foreign-*hacker*s-stole-240_n_899304.html. Acesso: 20 de novembro de 2013.

92 A estratégia de segurança cibernética dos Estados Unidos pode ser lida em http://www.defense.gov/news/d20110714cyber.pdf.

93 Batalha naval é um jogo de tabuleiro para dois jogadores, no qual os jogadores devem adivinhar em quais quadrados se encontram os navios do oponente. O objetivo da batalha naval é derrubar todos os navios do adversário. Os *hackers* que trabalham defedendendo e/ou atacando sistemas de governos e corporações devem estudar quais são os pontos fracos dos sistemas e redes para tentar invadi-los e/ou defendê-los.

No entanto, não é possível esperar que jovens passem por uma formação completa para poder ocupar as posições de cibersegurança que os EUA precisam. O *hacker* Johnny Long disse ao *Huffington Post* que o ideal é "o governo baixar os requisitos educacionais e recrutar pessoas baseadas somente nas suas habilidades como *hacker*s"[94]. Sem discriminação, como manda a ética *hacker*.

Outro problema para o recrutamento deste exército cibernético americano advêm das próprias normas de segurança federal. Muitos *hacker*s têm passagem pela justiça por invasão de sistemas de bancos, empresas e até mesmo do governo. Assim, a burocracia não permite que eles tenham acesso a determinados níveis de segurança, mesmo que dependam deles para trabalhar. Fazendo uma analogia com Michel Foucault em Vigiar e Punir, para se colocar na torre do ciber-panóptico que vai vigiar o mundo, os Estados Unidos precisam desconstruir seu panóptico interno e reconsiderar o passado dos *hackers* que deseja recrutar.

Finalmente, quando um *hacker* supera ideologias e passa por toda a burocracia necessária para ter acesso aos sistemas e programas que precisa para defender seu país de ataques cibernéticos das nações inimigas, ele vai ter que encarar o maior desafio previsto nessa mudança de ares: o trabalho. Jonathan Ripshy Duncan trabalhou para uma empresa que prestava serviços ao governo e não aguentou a rotina porque seu trabalho era "exatamente a mesma coisa todos os dias"[95]. A ética de trabalho *hacker* não faz com que eles fiquem confortáveis tendo que estar num escritório em horário comercial, seguindo regras e padrões que se repetem indefinidamente e tendo que reportar qualquer anormalidade. Os *hackers* trabalham em horários e locais de sua preferência e, mais importante, seu trabalho é a anormalidade. Quando tudo está seguindo um padrão, não há trabalho.

Além de todos os problemas éticos e ideológicos da relação *hackers*-governo, o esquema de espionagem da NSA aumentou o ruído que já existia e impediu uma maior aproximação entre as duas partes.

5.1. A NSA

A Agência de Segurança Nacional, NSA na sigla em inglês, é uma agência de segurança dos Estados Unidos especializada em produção e gerenciamento de *signals intelligence* (SIGINT), que é a coleta de informações através de interceptação de sinais de

94http://www.huffingtonpost.com/2011/08/08/government-recruits-*hacker*s-cyber-shortage_n_920795.html. Acesso: 20 de novembro de 2013.
95 Ibidem.

comunicação. Hoje, a SIGINT domina as ações de agências de inteligência e espionagem em todo o mundo, deixando a *human intelligence* (HUMINT) em segundo plano. A SIGINT trabalha com dados encriptados e análise de tráfego entre pessoas (*communications intelligence* – COMINT), sinais eletrônicos (*eletronic intelligence* – ELEINT) e uma combinação dos dois.

A NSA foi criada em 1952 pelo presidente Harry Truman e toda a documentação que oficializou sua criação era ultra-secreta[96], por isso, ficou conhecida à época como "*No Such Agency*" (Agência Inexistente) e "*Never Say Anything*" (Nunca Diga Nada)[97]. A NSA tem permissão para utilizar meios clandestinos e grampear meios de comunicação para alcançar seus objetivos e tem um dos maiores orçamentos e quadros de pessoal entre as agências norte-americanas.

O jornal Washington Post publicou no dia 29 de agosto de 2013 uma reportagem sobre o "*Black Budget*" (Orçamento Negro), que é o detalhamento de como o governo dos Estados Unidos distribui dinheiro entre as agências de inteligência e espionagem[98]. Apesar de sempre divulgar anualmente quanto gasta com estas agências, os EUA nunca especificaram como o dinheiro é dividido e utilizado. De acordo com a documentação obtida com Edward Snowden, ex-funcionário da NSA que terá um subcapítulo dedicado a ele neste trabalho, a NSA recebeu US$ 10,8 bilhões somente em 2013, 54% a mais do que o orçamento da agência em 2004. Quase metade da verba foi destinada a gerenciamento, instalações e suporte. A outra metade foi dividida para os custos de coleta, processamento, exploração e análise de dados. Isso mostra que a NSA tinha planos para expandir sua área de atuação, pelo menos até as denúncias feitas por Snowden ao jornal The Guardian em junho de 2013, de que a agência estava coletando dados telefônicos de cidadãos norte-americanos[99].

A informação divulgada pelo jornal britânico de que a companhia telefônica Verizon estava repassando para a NSA informações como números telefônicos, durações de chamadas e localização de pessoas comuns, que não necessariamente são suspeitas de terrorismo, abalou a imagem da agência e do governo Barack Obama. Ainda em junho, o Washington Post revelou que a NSA também coletava dados e fazia a vigilância de comunicações de nove

96 O memorando de criação da NSA pode ser acessado em: http://www.nsa.gov/public_info/_files/truman/truman_memo.pdf

97 http://www.thesundaytimes.co.uk/sto/news/world_news/Americas/article1271197.ece. Acesso: 23 de novembro de 2013.

98 http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html. Acesso: 23 de novembro de 2013.

99 http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Acesso: 23 de dezembro de 2013.

empresas de internet dos Estados Unidos através do programa de espionagem PRISM[100]. As empresas são: *Microsoft*, *Google*, *Facebook*, *Yahoo!*, *Apple*, *YouTube*, *AOL*, *Paltalk* e *Skype*. A *PalTalk* é a única empresa que não é tão importante quanto as outras, mas ela possui informações relevantes sobre a Primavera Árabe e guerra civil da Síria. Apesar das companhias negarem colaboração com o governo para divulgação de informações confidenciais dos usuários dos seus serviços, o debate sobre quais tipos de dados devem ou não devem ser armazenados e divulgados voltou à tona.

Desde junho, estão sendo divulgadas novas informações sobre a NSA – como as espionagens realizadas com cidadãos do Reino Unido, França e Alemanha, as tecnologias utilizadas pela agência para coletar e analisar estes dados e as respostas do governo às críticas que vem recebendo[101]. Em novembro de 2013, a NSA admitiu a um tribunal de inteligência ter cometido violações por "mau gerenciamento, falta de envolvimento por autoridades e falta de verificação dos procedimentos internos, e não por má fé"[102].

A vigilância e coleta de dados sem autorização judicial de pessoas que não são suspeitas de terrorismo fez com que a comunidade *hacker* se manifestasse contra a NSA. As aproximações que ocorreram nos últimos anos e o esforço feito pelo governo norte-americano para recrutar *hackers* para suas agências federais foram esquecidas a partir do momento em que as liberdades individuais foram atacadas. A liberdade e o direito à manter dados privados em sigilo são questões que estão no cerne da ética *hacker*. Como a NSA não mostrou apreço por essas questões, os *hackers* resolveram se afastar do governo norte americano. Para Alex Stamos, especialista em segurança da informação que palestrou na DEFCON 2013, "houve um retrocesso de cerca de 10 anos entre os 'mocinhos' e o governo dos Estados Unidos".

O jornalista Joseph Menn, da Reuters, cobriu a DEFCON e a Black Hat – outra conferência de segurança da informação, mas que reúne grandes empresas e profissionais bem-sucedidos do ramo – e mostrou que os jovens *hacker*s e ativistas que estiveram na DEFCON estão decepcionados com a espionagem do governo americano, enquanto empresários e especialistas em segurança ainda consideram trabalhar para uma agência

100http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html. Acesso: 23 de novembro de 2013.

101 A Electronic Frontier Foundation mantem em sua página na internet uma linha do tempo com os acontecimentos mais importantes sobre a espionagem praticada pela NSA, com reportagens, artigos e informações oficiais do tribunal que está supervisionando o caso. A linha do tempo é constantemente atualizada e pode ser acessada em: https://www.eff.org/nsa-spying/timeline.

102 http://exame.abril.com.br/mundo/noticias/eua-publicam-documentos-sobre-programa-da-nsa. Acesso: 23 de novembro de 2013.

federal[103]. Jeff Moss, fundados dos dois eventos, diz que "nunca viu tanta animosidade desde os anos 90", quando *hackers* eram tratados basicamente como ladrões e não se considerava a importância da comunidade para o desenvolvimento de novas tecnologias e avanços na área de segurança da informação. No entanto, Moss vê com certo otimismo os acontecimentos recentes porque "antes do vazamento de informações pelo Snowden, era impossível ter uma discussão bem informada sobre como balancear segurança e liberdades civis sem o real conhecimento das práticas governamentais"[104].

5.2. O caso Edward Snowden

Edward Snowden é um ex-funcionário da NSA, onde trabalhava como analista de inteligência responsável pelo vazamento de informações de que a agência espionava ligações e e-mails de milhões de pessoas, além de informações diplomáticas, políticas e econômicas de outros países[105]. A empreitada de Snowden começou no dia 20 de maio de 2013, quando ele viajou para Hong Kong e se preparou para revelar tudo que sabia sobre as atividades da Agência de Segurança Nacional dos Estados Unidos deixando para trás sua família e o que ele classificaria posteriormente de "vida muito confortável" quando revelou sua identidade. No dia 05 de junho o jornalista Glenn Greenwald publicou no The Guardian uma matéria sobre a coleta de dados de ligações telefônicas de norte-americanos. Hoje Snowden vive na Rússia, onde obteve asilo político temporário. Ele enviou pedido de asilo a diversos países, inclusive ao Brasil[106].

Mas o que levou um especialista em informática e segurança da informação, com alto grau de acesso a dados confidenciais, a resolver denunciar tudo que estava sendo feito pelo seu próprio governo? "Meu único motivo é informar às pessoas sobre o que é feito em seus nomes e que isso é feito contra eles"[107]. Snowden se alistou no exército para lutar na Guerra do Iraque porque "sentia a obrigação como ser humano de libertar as pessoas da opressão"[108]. As duas falas do delator revelam um senso de justiça e de verdade inerentes à Ética *Hacker* de

---

103 http://www.reuters.com/article/2013/08/03/net-us-usa-security-hacking-ethics-idUSBRE9720A020130803. Acesso: 23 de novembro de 2013.
104 Ibidem. Tradução nossa.
105 A página em inglês da Al Jazeera, maior emissora de televisão jornalística do Catar, mantem uma linha do tempo sobre as revelações feitas por Edward Snowden e suas consequências com notícias de diversos veículos do mundo. A linha do tempo é constantemente atualizada e pode ser acessada em: http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html.
106 http://wikileaks.org/Edward-Snowden-submits-asylum.html. Acesso: 26 de novembro de 2013.
107 http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance: Acesso: 26 de novembro de 2013.
108 Ibidem.

Steven Levy. O que Snowden fez foi desconfiar de autoridades e tornar certas informações livres, descentralizando a posse delas das mãos do governo. Ele revela ao The Guardian que também não quer viver em um mundo no qual não possa acessar a internet sem ter certeza de que terá total privacidade para navegar, trocar mensagens e explorar sua criatividade.

Ao agir sob os preceitos da ética *hacker*, Snowden foi acusado de roubo, comunicação não autorizada de informação da defesa nacional e comunicação intencional de informações confidenciais de inteligência para pessoa não autorizada. As duas últimas acusações foram feitas sob o Ato de Espionagem de 1917[109]. Os jornalistas Glenn Greenwald e Laura Poitras, as únicas pessoas além de Snowden que também têm acesso à documentação da NSA, também estão sofrendo perseguição do governo norte-americano. Em agosto de 2013, o brasileiro David Miranda, companheiro de Greenwald, foi detido no aeroporto de Heatrow, em Londres, baseado no Ato de Terrorismo do Reino Unido[110]. O Ato permite que a polícia britânica detenha uma pessoa em um porto, aeroporto ou fronteira por até nove horas para interrogá-la sobre envolvimento em atividades terroristas. Os Estados Unidos admitiram que o Reino Unido estava fazendo um alerta a Greenwald, mas que não estavam envolvidos na ação[111].

O que é mais contraditório, e até mesmo curioso, em todo o caso de Edward Snowden e a delação da espionagem praticada pela NSA é que ele era considerado um "*hacker* ético" pela própria agência federal. Ele possui o Certificado de *Hacker* Ético do *Internet Council of E-Commerce Consultants* (*EC-Council*)[112]. Para o *EC-Council*, um *hacker* ético é a pessoa preparada para proteger sistemas de informações e consertar problemas que facilitem a invasão. Na página do *EC-Council* eles dizem que "para vencer um *hacker*, você precisa pensar como eles", mostrando que para a empresa – e consequentemente para o governo e a NSA que aceitam o certificado para seus funcionários – um *hacker* nada mais é que um criminoso que invariavelmente só invade sistemas em busca de informações confidenciais que serão usadas de forma indevida. A procura das agências federais por *hackers* não aconteceu porque houve uma mudança de mentalidade em relação aos *hacker*s tão profunda quanto acreditava-se ter havido. Edward Snowden criou um novo problema para os poderes estabelecidos: além de temer os *hackers*, eles devem também temer a população que cada vez

109 http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html. Acesso: 26 de novembro de 2013.
110 http://www.nytimes.com/2013/08/19/world/europe/britain-detains-partner-of-reporter-tied-to-leaks.html. Acesso: 26 de novembro de 2013.
111 http://www.bbc.co.uk/news/uk-23761918. Acesso: 26 de novembro de 2013.
112 http://mashable.com/2013/07/05/snowden-ethical-*hacker*. Acesso: 26 de novembro de 2013.

mais quer proteger seus dados privados e saber onde estão os dados que deveriam ser públicos. No dia 1º de julho de 2013, Snowden falou sobre o assunto:

> No fim, o governo Obama não teme delatores como eu, Bradley Manning ou Thomas Drake. Nós somos apátridas, prisioneiros ou impotentes. Não, o governo obama teme você. Ele teme uma população furiosa, informada, exigindo o governo constitucional que lhes foi prometido - e que deveria ser.[113]

5.3. Espionagem e vazamento de dados no Brasil

Ao longo do segundo semestre de 2013 mais informações sobre a espionagem da NSA foram reveladas. A agência também interceptava dados de outros países, não só dos Estados Unidos. Algumas das que sofreram com a vigilância dos Estados Unidos foram a Rússia, China, Irã, Paquistão, França, Espanha, México e Brasil, com a justificativa de que estavam procurando por atividades terroristas e/ou informações econômicas que evitassem uma nova crise mundial.

As primeiras informações de que o Brasil foi alvo da espionagem americana foram reveladas no dia 06 de julho de 2013 pelo jornal O Globo em parceria com Glenn Greenwald, que forneceu acesso aos documentos de Edward Snowden[114]. Apesar da falta de números precisos, estima-se que milhões de pessoas tiveram suas ligações telefônicas e e-mails interceptados, fazendo do país uma das nações mais vigiadas pela NSA e o território mais visado da América do Sul pela inteligência norte-americana. A reportagem d'O Globo revelou o uso de outro programa pela NSA além do *Prism*. O *Fairview* é o *software* responsável pela espionagem fora do território americano. Sob a ordem presidencial 12333, que dá poderes à agência para vigiar pessoas, empresas e governos estrangeiros, a NSA consegue tornar a espionagem no Brasil tão simples de ser realizada quanto é em seu próprio território.

Em setembro de 2013 vieram à tona as informações de que Dilma Rousseff foi um alvo específico da vigilância eletrônica da NSA. Uma apresentação obtida por Edward Snowden e que chegou às mãos de Glenn Greenwald mostra como mensagens da presidenta para seus assessores e também do presidente do México, Peña Nieto – então candidato ao

113 http://wikileaks.org/Statement-from-Edward-Snowden-in.html. Acesso: 26 de novembro de 2013.
114 http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934. Acesso: 27 de novembro de 2013.

cargo –, para aliados foram interceptadas e decodificadas[115]. Com o título "Filtragem inteligente de dados: estudo de caso México e Brasil", a apresentação mostra como o uso de três programas – *Mainway, Association e Dishfire* – podem "achar agulha no palheiro". O primeiro *software* é responsável pela coleta do grande volume de informações que passa pelas redes de comunicação, o segundo filtra mensagens de texto enviadas pelos celulares e o terceiro programa faz a busca por palavras-chave específicas nos dados interceptados. Uma parte da apresentação tem o título "mensagens interessantes" e mostra mensagens de texto enviadas por Peña Nieto falando sobre seus futuros assessores caso vencesse a eleição. Hoje, os nomes citados estão ocupando cargos no governo mexicano[116].

No mesmo mês em que foi revelada espionagem à Dilma Rousseff, o programa televisivo Fantástico mostrou que a Petrobras também foi alvo da NSA, revelando um esquema de espionagem estratégica e econômica promovido pelos Estados Unidos[117]. Em outra apresentação da agência, dessa vez para treinar novos agentes no acesso à redes de segurança de empresas, governos e bancos, o nome da Petrobras aparece diversas vezes, assim como do *Google* – que foi acusado de colaborar com a NSA na utilização do *Prism* –, do Ministério das Relações Exteriores da França e da rede bancária *Swift*, responsável por controlar transações financeiras internacionais realizadas por telecomunicações.

Na apresentação são mostrados documentos da agência de espionagem da Inglaterra, a GCHQ, que trabalha com a NSA e as agências do Canadá, Austrália e Nova Zelândia, formando o grupo *Five Eyes* (cinco olhos). A CSEC, agência de inteligência canadense, também espionou o Brasil. Em uma conferência de analistas do Five Eyes foi mostrado como o programa Olympia mapeou ligações telefônicas e trocas de mensagens realizadas pelo Ministério de Minas e Energia[118].

Fica claro que o interesse da espionagem do *Five Eyes* no Brasil não é apenas o combate ao terrorismo, mas também a procura por informações estratégicas, políticas e econômicas do governo brasileiro, principalmente no setor de energia. Em 2009, Thomas Shannon, então subsecretário do Departamento de Estado norte-americano e hoje embaixador dos Estados Unidos no Brasil, enviou uma carta à NSA agradecendo a agência pelas

115 http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html. Acesso: 27 de novembro de 2013.
116 A apresentação pode ser acessada em: http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html
117 http://g1.globo.com/fantastico/noticia/2013/09/petrobras-foi-espionada-pelos-eua-apontam-documentos-da-nsa.html. Acesso: 27 de novembro de 2013.
118 http://g1.globo.com/fantastico/noticia/2013/10/ministerio-das-minas-e-energia-esta-na-mira-de-espioes-americanos-e-canadenses.html. Acesso: 27 de novembro de 2013.

informações captadas às vésperas da 5ª Cúpula das Américas, que aconteceu em Trinidad e Tobago em abril daquele ano, dando vantagem ao presidente Barack Obama na discussão de assuntos sensíveis com países como Brasil, Venezuela e Bolívia.. Shannon escreveu agradecendo aos

> […] mais de 100 relatórios que recebemos da agência (que) nos deram uma compreensão profunda dos planos e intenções dos outros participantes da cúpula e permitiram que nossos diplomatas estivessem bem preparados para aconselhar o presidente Obama em como lidar com questões controversas, tais como Cuba, e interagir com contrapartes difíceis, como o presidente venezuelano Hugo Chávez.[119]

Durante a Assembleia Geral das Nações Unidas, que aconteceu no dia 24 de setembro de 2013, em Nova York, Dilma Rousseff condenou a espionagem realizada pela NSA, afirmando que ela fere a soberania do Brasil e de outros países que tiveram suas comunicações vigiadas. Para a presidenta do Brasil, espionar cidadãos fere direitos humanos e liberdades civis – ponto que já foi atacado por Snowden ao revelar sua motivação para delatar a NSA – e vigiar governos e empresas vai contra a soberania das nações[120].

119 http://epoca.globo.com/tempo/noticia/2013/08/carta-em-que-o-atual-bembaixadorb-americano-no-brasil-bagradece-o-apoio-da-nsab.html. Acesso: 27 de novembro de 2013.
120 O discurso completo de Dilma Rousseff na Assembleia Geral da ONU pode ser acessado em: http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

6. CONSIDERAÇÕES FINAIS

A temática da ética se fez presente ao longo deste trabalho. Tanto explicitamente, quando falávamos diretamente a respeito de suas implicações e influências na cultura *hacker*, quanto implicitamente, em discussões sobre atitudes engendradas por *hackers* em atos de espionagem e quebra de segurança. No entanto, percebe-se que a ética só foi um tema porque o ponto principal discutido neste estudo foi o trabalho. A Ética *Hacker* nada mais é do que uma alternativa à ética do trabalho proposta por Max Weber em sua obra "A ética protestante e o espírito do capitalismo".

Quando Pekka Himanen (2001) diz que a ética do trabalho *hacker* é um contraponto a ética protestante, é possível afirmar que ele teve a "infelicidade" de lançar sua obra no ano de 2001, exatamente na virada do século e do milênio, época marcada por grandes mudanças no rumo da História. Além da importância da mudança de década, século e milênio, os ataques terroristas de 11 de setembro de 2001 aceleraram por alterações drásticas na sociedade, Economia e no pensamento contemporâneo. Envolvem aspectos fundamentais para o modo como vemos a tecnologia atualmente.

Himanen (2001) vê a Ética *Hacker* como uma evolução da ética capitalista de Weber, no entanto o capitalismo ganhou força com o desenvolvimento da tecnologia e da internet no início do século 21, relegando o pensamento libertário dos *hackers* a segundo plano. A ideia de que poderíamos fazer nossos próprios horários de trabalho e que não precisaríamos nos reportar a um superior continuou tão fantasiosa quanto a dos *hackers* retratados nos filmes em que gangues de piratas virtuais roubavam milhões de dólares de bancos com facilidade utilizando *softwares* de visual futurista.

A teoria de Manuel Castells (2000) de que o trabalho continuaria a ser o centro da vida do ser humano se confirmou e a preponderância dos interesses econômicos e financeiros das grandes corporações pressionando lideranças políticas mantidas por elas estão fazendo com que a centralidade humanística e o método científico sejam deixados de lado em prol da velocidade da criação e do lucro. É preciso repensar o tipo de profissional que está sendo formado e entrando no mercado de trabalho. Não só na área da informática e tecnologia da informação, mas em todos os campos de conhecimento. É preciso que todos sejamos um pouco *hackers* como propôs Pablo Mancini (2011), e reprogramemos os escritórios e os produtos resultantes do trabalho. Dentro do jornalismo, que é a área de estudo de Mancini, ele traz exemplos de como a Ética *Hacker* ainda pode existir e se destacar nestes tempos.

Iniciativas como o portal de notícias *Newser*[121] e o *WikiLeaks*, que foi um dos objetos de estudo deste trabalho, são exemplos das tendências do jornalismo contemporâneo. O primeiro sumariza notícias de outros grandes portais e adiciona pequenos comentários sobre o assunto em pauta, sempre indicando o caminho para o leitor acessar a matéria original. Já o WikiLeaks através de técnicas de programação e segurança da informação para proteger seus servidores e com o apoio de espiões e pessoas com acesso a informações confidenciais de governos e corporações, torna públicas informações que são de interesse de todos ao mesmo tempo que oferece pautas prontas para grandes veículos de comunicação.

Os incentivos ao ensino da programação e das linguagens de códigos desde os primeiros anos escolares ainda não mostraram se querem revolucionar as relações de trabalho ou criar *hackers* que tenham afinidade com os governos e os poderes estabelecidos. O crescente interesse de governos por sistemas de segurança, espionagem, *data mining* e *big data* coloca os *hackers* novamente no centro da discussão sobre o trabalho. Na era da Economia Informacional, em que dados e informações valem muito dinheiro e podem iniciar ou terminar guerras, os *hackers* são essenciais para defender sistemas de ataques de nações inimigas, não deixar a guerra ao terror perder força e recolher dados pessoais de indivíduos livres de suspeitas e governantes e também de empresas para ajudar governos a traçar suas estratégias econômicas e diplomáticas dos próximos anos. Quando estes *hackers* se dão conta de que não podem viver ao mesmo tempo sob a regência da ética protestante deste "capitalismo informacional" e da ética *hacker* acontecem denúncias como as que foram protagonizadas por Edward Snowden, insatisfeito com os rumos que seu trabalho havia tomado e por ajudar a invadir a privacidade de milhões de pessoas diariamente.

Este trabalho se propôs a estudar as relações de trabalho dos *hackers* desde o surgimento de sua cultura própria, no início dos anos 60 no MIT, até o que é feito hoje para manter vivo seu espírito ético numa época de tecnologia altamente desenvolvida e de falta de privacidade. Em que momentos da História os hackers deixaram de ser vistos como criminosos e se tornaram figuras essenciais para a Era da Informação? Eles realmente deixaram para trás esta pecha de criminosos ou esta visão varia de acordo com aquilo que convém aos grupos interessados? A Ética *Hacker* poderá suplantar a ética capitalista em algum momento ou terá que andar sempre paralelamente e a margem dela?

Entende-se que novos estudos e pesquisas devem continuar acompanhando o desenrolar das denúncias de espionagem feitas por Edward Snowden, visto que é um processo

[121] http://www.newser.com. Acesso em: 02 de dezembro de 2013.

ainda em andamento e que certamente irá gerar bibliografia especializada acerca da Ética *Hacker* e do direito à liberdade e privacidade e da necessidade de trazer a tona dados de interesse público, como informações governamentais e corporativas.

7. REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSON, Chris. **The end of theory: the data deluge makes the scientific method obsolete**. 2008. Disponível em: www.wired.com/science/discoveries/magazine/16-07/pb_theory. Acesso: 02 de novembro de 2013.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2000.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Petrópolis: Vozes, 2009.

GILMORE, John. **Privacy, technology and the open society**. 1991. Disponível em: http://www.toad.com/gnu/cfp.talk.txt. Acesso: 02 de dezembro de 2013.

HIMANEN, Pekka. **The hacker ethic and the spirit of the information age**. Nova York: Random House, 2001.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

_____. **O Que é Virtual**?. Rio de Janeiro: Editora 34, 1996.

LEVY, Steven. **Hackers: Heroes of Computer Revolution**. Nova York: Doubleday, 1984.

MANCINI, Pablo. **Hackear el Periodismo: Manual de Laboratorio**. Buenos Aires: LaCrujia, 2011.

RAYMOND, Eric. **The art of unix programming**. Boston: Addison-Wesley, 2003.

_____. **The Cathedral and the bazaar**. California: O'Reilly Media, 1999.

_____. **The early hackers**. Disponível em: http://www.catb.org/esr/writings/homesteading/hacker-history/ar01s02.html. Acesso: 21 de setembro de 2013.

STALLMAN, Richard. **On hacking**. Disponível em: http://stallman.org/articles/on-hacking.html. Acesso: 21 de setembro de 2013.

_____. **The free software definition**. 2010. Disponível em: http://www.gnu.org/philosophy/free-sw.html. Acesso: 17 de novembro de 2013.

WEBER, Max. **A ética protestante e o espírito do capitalismo**. São Paulo: Martin Claret, 2009.